Dakota State University
Beadle Scholar

Masters Theses

Fall 12-1-2004

The Creation of a Distance Learning Graduate Level Course in Legal and Ethical Aspects of Technology

Wade M. Chumney
Dakota State University

Follow this and additional works at: https://scholar.dsu.edu/theses

Recommended Citation
Chumney, Wade M., "The Creation of a Distance Learning Graduate Level Course in Legal and Ethical Aspects of Technology" (2004). *Masters Theses*. 56.
https://scholar.dsu.edu/theses/56

This Thesis is brought to you for free and open access by Beadle Scholar. It has been accepted for inclusion in Masters Theses by an authorized administrator of Beadle Scholar. For more information, please contact repository@dsu.edu.

THE CREATION

OF A

DISTANCE LEARNING GRADUATE LEVEL COURSE

IN LEGAL AND ETHICAL

ASPECTS OF TECHNOLOGY

By

Wade M. Chumney

A Project Presented in Partial Fulfillment

Of the Requirements for

The Master of Science in Information Systems

At Dakota State University

December 2004

3513 Old Ferry Rd.
Johns Island, SC 29455
843-571-5290
wchumney@gmail.com

Committee Members:
Professor Mr. Mark Moran
Professor Mr. Rick Puetz
Professor Mr. Tom Farrell

MSIS
PROJECT APPROVAL FORM

Student Name: Wade M. Chumney

Expected Graduation Date: 12/04

Master's Project Title: Designing a Graduate Level Course entitled: Legal and Ethical Aspects of Managing Technology

Date Project Plan Approved: 6/04

Date Project Coordinator Notified and Grade Submitted: _____

Approvals/Signatures:

Student: Wade M. Chumney /s Date: 9/17/04

Faculty supervisor: Mark Nolan Date: 9/29/2004

Committee member: Richard O'Neill Date: 9-29-2004

Committee member: Tom Farrell Date: 9-29-2004

To Ensure Certification of Completion:
Student must bring or send the original to the Graduate Programs Office.
Copies on acid free paper go to the library with the reports for binding.

Original to Graduate Programs Office
Acid-free copies with written reports to library
Copies to: Project supervisor and committee and to MSIS Coordinator

Revised 1/28/03

Abstract

This goal of this project is to provide a quality graduate level distance learning course administered via WebCT that can be administered by a professor possessing a Juris Doctor. To accomplish this goal, two primary texts were selected: Ethics in Information Technology, by Reynolds, George (2003), published by Thomson Course Technology., ISBN: 0-619-06277-0 and CyberLaw: Text and Cases, 2nd edition, Ferrera, Gerald and Stephen Lichtenstein, and Margo Reder, and Robert Bird, and William Schiano (2004), published by Thomson (West Legal Studies in Business), ISBN: 0-324-16488-2. Additionally, a number of papers were written on issues pertinent to the class, several PowerPoint presentations dealing with Internet law were created, quizzes and tests were designed to measure student understanding, and a number of lectures on legal and ethical issues were recorded. Each of these components was incorporated into the WebCT class module to most effectively enhance the learning experience.

Table of Contents

List of Tables

List of Figures

Introduction

Accreditation agencies for graduate and undergraduate programs in the information technology field often require that students develop a knowledge and appreciation of ethical and legal components of technology. For instance, one of the premiere accrediting agencies, Accreditation Board for Engineering and Technology Computing Accreditation Commission (CAC/ABET) proposes the following Criteria for Accrediting Computer Programs which apply to computing programs using information technology or similar terms in their titles:

> 1. Objectives, Outcomes and Assessment
>
> ...
>
> (f) Analyze the impact of technology on individuals, organizations and society, including ethical, legal, security and global policy issues;[1]

Given these objectives, it is critical that students enrolled in a Masters Degree program in an information technology field take a course that addresses these issues. My goal in undertaking this project was to create such a course.

Statement of Problem Being Addressed

The issue being addressed by this project is the need for a broader understanding of the impact technology has within a social context, particularly the legal and ethical

[1] 2005-2006 Criteria for Accrediting Computing Programs – Proposed Changes. http://www.abet.org/criteria_cac.html

implications of technology. One cannot have a full understanding of information technology without being exposed to the numerous legal issues and ethical quandaries posed by the introduction of this science into society at large. It is for this reason that a number of accreditation agencies for technology-related programs, now require that legal and ethical aspects of technology be taught within established technology programs.

To provide this type of information to students, schools have chosen to take basically one of two routes. The first route some universities have chosen is to integrate a modest amount of legal and ethical teachings into each and every course offered in the technology-related program. This solution is beneficial because it does not require the creation of a totally new course and it can allow for a more pervasive exposure to these issues as students will encounter them in every technology course they take. This method also has downsides; the first is that the various professors may lack the knowledge and/or desire to properly teach these concepts. Secondly, only a dedicated course devoted exclusively to the legal and ethical aspects of technology allows for truly in-depth coverage of pertinent issues and concepts.

Weighing these advantages and disadvantages, it was deemed appropriate to take the second route that many universities have followed. This is to design a stand alone course from the ground up that deals with the various legal and ethical issues encountered by technology and those who use it. This method has proven effective as it appears to be the action taken by the majority of programs in the United States.

Objectives of the Project

The objective of this project is to create a graduate level distance learning course to be administered via WebCT that meets the proposed criteria established by the Accreditation Board for Engineering and Technology Computing Accreditation Commission (CAC/ABET). To meet this goal, a number of elements were incorporated within the WebCT framework. These elements include: PowerPoint presentations, quizzes and tests, issue-specific writings, and recorded live lectures.

PowerPoint Presentations

It is my belief that PowerPoint presentations provide a critical component to the online learning experience. As such, three different sources of PowerPoint presentations were utilized. The first two sets were those primarily prepared by the authors of the two primary texts for the course: Ethics in Information Technology, by George Reynolds CyberLaw: Text and Cases, by Gerald Ferrera and Stephen Lichtenstein, and Margo Reder, and Robert Bird, and William Schiano. These presentations were reviewed and minor modifications were made. The final set of PowerPoint presentations are those self-designed for use in the course. Four topics were chosen that were critical to the understanding of the legal aspects of technology: 1) Internet Jurisdiction and 2) Intellectual Property issues on the Internet 3) Defamation, Right of Publicity, and Privacy on the Internet, and 4) Legal Issues in E-Commerce. Each of these was designed from the ground up using knowledge of the issues and numerous legal sources.

Quizzes and Tests

These knowledge assessment tools provide a necessary means to gauge student learning. As with the first two sets of PowerPoints, two sources were those provided by the authors of the texts. In addition, self-made test questions were incorporated on issues in which it was critical to have the students relate their knowledge in a coherent written product.

Issue-Specific Writings

The topics for these learning components were chosen based upon areas which needed further explanation from the student's perspective. Six topics were chosen on which to provide further information to the students: 1) Internet Domain Names, 2) Intellectual Property Assets, 3) The Open Source Movement, 4) Internet Use Policies, 5) E-Commerce, and 6) Cybersecurity. These writings will provide the students with the background they need to better understand the legal and ethical issues related to those aspects of technology in today's society.

Recorded Live Lectures

In addition to the aforementioned components of my graduate level course, two separate hour long presentations were given on two critical topics in order to assist student learning. The first of these lectures dealt with Internet Jurisdiction. A case study was presented of how Internet jurisdiction is determined in the Fourth Circuit (coincidentally, it is in line with most Circuits in the U.S.). This lecture will greatly assist students in understanding the determining factors that decide where an entity that

conducts business via the Internet can be subject to legal action. The second hour long lecture deals with the critical topic of Intellectual Property Issues on the Internet. There is a tremendous amount of material on this topic and it was important to present this information to the students in a coherent, manageable package because these concepts form the foundation for how the Internet is regulated by our legal system.

Scope of the Project

To accomplish these goals extensive research was conducted into several areas of the law and ethics of technology. The first task was to decide which textbooks would provide the foundation for this learning experience. An extensive literature review was conducted and ultimately each of the following texts was considered for the course:

CyberEthics: Morality and Law in Cyberspace by Richard Spinello

Technology Lost: Hype and Reality in the Digital Age by Ron Schneiderman

Ethics in Information Technology by George Reynolds

Case Studies in Information Technology Ethics by Richard Spinello

Computers and Ethics in the Cyberage by Micah Hester and Paul Ford

Ethics in the Information Age by Michael Quinn

Morality and Machines by Stacey Edgar

CyberEthics by Terry Halbert and Elaine Infulli

Legal Land Mines in E-Commerce by David Canton and John Millar

Legal Aspects of Managing Technology by Lee Burgunder

Readings in CyberEthics by Richard Spinello and Herman Tavani

CyberLaw: Text and Cases by Gerald Ferrera, Stephen Lichtenstein, Margo Reder, Robert Bird, and William Schiano

It was originally conceived that one text would be chose that covered all the concepts sufficiently, but ultimately two texts were chosen that expertly covered the two critical aspects of the course: the law of technology, and the law of ethics. The two textbooks chosen were CyberLaw: Text and Cases by Gerald Ferrera, et. al. and Ethics in Information Technology by George Reynolds.

The second task was to create a syllabus which would provide the framework upon which student learning would be built. In order to do this, the researcher's knowledge of the subject matter, the material chosen for the legal aspects of the course, and the material chosen for the ethical aspects of the course all had to be synthesized. The number of course meetings is based upon the researcher's fall semester experience at Dakota State University. That construct provided for six class sessions of four hours, one two hour class session immediately followed by a midterm exam, and one additional class period for the final exam. The breakdown for coverage of the material during that time frame is set out in the course syllabus.

Table 1: Syllabus for Legal and Ethical Aspects of Technology

Week	Date (Wed.)	Topic	Readings
2	Sept. 8	- Course introduction	
		- Ethics Overview	(EIT)Ch.1
		- Ethics for IT Professionals and IT Users	(EIT)Ch.2
		- Technology and CyberLaw	(CL)Ch.1
		- Jurisdiction	(CL)Ch.2
		-Jurisdiction Case Study	PP and Recorded Lecture
4.	Sept. 22	- Intellectual Property Overview	(EIT)Ch.6
		- Trademarks	(CL)Ch.3
		- Internet Domain Names	Handout
6	Oct. 6	- Copyrights	(CL)Ch.4
		- Business Method Patents and Trade Secrets	(CL)Ch.5
		- Intellectual Property as a Business Asset	Handout
8	Oct. 20	- Intellectual Property Issues on the Internet	PP and Recorded Lecture
		- Open Source	Handout
		(Wed., Oct 20, 8:00-10:00PM, Midterm Exam)	
10	Nov. 3	- Software Development	(EIT)Ch.7
		- Employer/Employee Issues	(EIT)Ch.8
		- Online Contracting	(CL)Ch.6
		- E-mail and Internet Use Issues	Handouts
		- E-Commerce Overview	Handout
		-E-Commerce	PowerPoint
12	Nov. 17	- Privacy	(EIT)Ch.4 and (CL) Ch.9
		- Freedom of Expression	(EIT)Ch.5
		- Obscenity	(CL)Ch.10
		- Defamation	(CL)Ch.11
		-Defamation, Right of Publicity, and Privacy	PowerPoint
14	Dec. 1	- Computer and Internet Crime	(EIT)Ch.3, (CL) Ch.13
		- Internet and Information Security	(CL)Ch.12
		- CyberSecurity	Handout
		- Review	
16	Dec. 15	Final Exam	
		(Wed., Dec. 15, 6:00 – 10:00PM, Final Exam)	

* **(EIT):** Ethics in Information Technology textbook; **(CL):** CyberLaw textbook

With the syllabus firmly established, four areas were chosen in which to create PowerPoint presentations for the course: 1) Jurisdiction on the Internet, 2) Intellectual Property Law on the Internet, 3) Defamation, Right of Publicity, and Privacy on the Internet, and 4) Legal Issues in E-Commerce. For two of these presentations, Jurisdiction on the Internet and Intellectual Property Law on the Internet, live audio lectures of the materials were recorded and incorporated them into the WebCT course. In addition, six topics considered to be critical to the course were chosen and papers were written on each summarizing the key concepts. These topics included: 1) Internet Domain Names, 2) Intellectual Property Assets, 3) The Open Source Movement, 4) Internet Use Policies, 5) E-Commerce, and 6) Cybersecurity. In this section, the PowerPoints and papers that were researched and created for the course are presented.

PowerPoint Presentation Regarding Personal Jurisdiction on the Internet: A Case Study of the Fourth Circuit

Personal Jurisdiction on the Internet: A Case Study of the Fourth Circuit

Wade M. Chumney, Esq.

Personal Jurisdiction and Related Issues

●Implications of the Internet

–allows businesses to reach a wide audience without incurring significant start-up costs or investment of time.

–Consequently, small businesses with minimal capital are able to function on the Internet but are unable to afford the costs of litigating matters throughout the country.

–The logical conclusion is that many businesses, especially small ones, would be discouraged from obtaining an Internet presence when doing so would subject them to nationwide jurisdiction

●Some suggest that a new, unique analysis for assessing personal jurisdiction over the Internet should be devised

●Others argue that the traditional framework can adequately address the issue and that the Internet is no different from other increases in technology in the twentieth century that led the Supreme Court to its decision in International Shoe

●Until the Supreme Court addresses this issue or some other federal action is taken, courts must apply the traditional due process analysis in suits involving Internet contacts

Jurisdiction in a Traditional Setting

●General Jurisdiction

–State's "enduring relationship" jurisdictional statute, a South Carolina court may exercise personal jurisdiction over a person

•Domiciled in

•Organized under the laws of,

•Doing business

•Maintaining his or her principal place of business in

–This State as to any cause of action

–Similarly, federal due process cases acknowledge that a court may exercise general jurisdiction over a defendant whose contacts with the forum state are "continuous and systematic."

Jurisdiction in a Traditional Setting

•Specific Jurisdiction

•The South Carolina long-arm statute provides the statutory basis for asserting specific jurisdiction in this state:

•(1) A court may exercise personal jurisdiction over a person who acts directly or by an agent as to a cause of action arising from the person's

–(a) transacting any business in this State;

–(b) contracting to supply services or things in the State;

–(c) commission of a tortious act in whole or in part in this State;

–(d) causing tortious injury or death in this State by an act or omission outside this State if he regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered, in this State; or

–(e) having an interest in, using, or possessing real property in this State; or

–(f) contracting to insure any person, property or risk located within this State at the time of contracting; or

–(g) entry into a contract to be performed in whole or in part by either party in this State; or

–(h) production, manufacture, or distribution of goods with the reasonable expectation that those goods are to be used or consumed in this State and are so used or consumed.

Jurisdiction in a Traditional Setting

- The determination of whether a court may exercise personal jurisdiction over a non-resident under the long-arm statute involves a two-step analysis.
- First, the trial judge must determine that the South Carolina long-arm statute applies.
- Second, the trial judge must determine that the nonresident's contacts in South Carolina are sufficient to satisfy due process requirements.

–Since the South Carolina Long Arm statute has been interpreted as extending to the limits of due process, the statutory inquiry necessarily merges with the Constitutional inquiry.

–Therefore, the question is whether exercising personal jurisdiction over the defendant violates due process.

Jurisdiction in a Traditional Setting

- Because a state's judicial power only extends within its borders, the "defendant's contacts with the foreign state [must be] so substantial that they amount to a surrogate for presence and thus render the exercise of sovereignty just, notwithstanding the lack of physical presence in the state."

●Thus, the court must find that the defendant:

–1) Has minimum contacts with the foreign state, and

–2) That the exercise of jurisdiction comports with notions of fair play and substantial justice.

Jurisdiction in a Traditional Setting

●"Minimum Contacts"

–Focus must center on the contacts generated by the defendant, and not on the unilateral actions of some other entity.

–Defendant must purposefully avail itself of the privilege of conducting activities in the forum state, thus invoking the benefits and protections of its laws.

–Defendant will not be haled into a jurisdiction solely as the result of random, isolated, fortuitous or attenuated contacts.

Jurisdiction in a Traditional Setting

●The second prong of the due-process analysis in determining whether personal jurisdiction should be exercised is whether the assertion of such jurisdiction comports with fair play and substantial justice.

–Burdens on the plaintiff

–Burdens on the defendant

–Interest of the states involved

–Efficiency of resolving litigation

Jurisdiction Over Activities on the Internet

●Emergence of the Internet

●Traditional jurisdiction framework is being forced to handle a novel set of issues with regard to personal jurisdiction.

●Traditional framework was developed when "jurisdictional lines followed state boundaries, and parties more clearly understood the scope of their jurisdiction as well as the location of other parties with whom they were transacting."

●Cyberspace

–a world without traditional boundaries where businesses and individuals conduct transactions without knowledge of each other's physical location.

Jurisdiction Over Activities on the Internet

●Zippo Manufacturing Co. v. Zippo Dot Com, Inc.

●W. District of PA, January 1997

●D filed Motion to Dismiss for Improper Venue and Transfer, and Motion to Dismiss for Lack of Personal Jurisdiction

●P Pennsylvania Corp. made Zippo lighters

●D Cal Corp. operated Internet News Service under Zippo.com, Zippo.net, and Zipponews.com

●2% of D's subscribers (3,000) were PA residents

●D entered into 7 contracts w/ PA ISPs for customers

●P alleged TM infringement, TM dilution, and other claims

●Issue: Constitutionally permissible reach of PA's Long Arm Statute through Cyberspace

●PA Contracts + PA Subscribers + Interactive Website = purposeful availment of doing business in PA

Jurisdiction Over Activities on the Internet

•Zippo Manufacturing Co. v. Zippo Dot Com, Inc.

–"Passive" Web sites in which the defendant has done nothing but advertise its product on the Internet. Most courts find personal jurisdiction cannot be exercised in these cases.

–"Interactive" Web sites whereby individuals enter into contracts with defendants via the Internet and download, transmit or exchange files. As is expected, courts have found personal jurisdiction proper in these cases.

–In between these two categories are Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.

•The "likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet."

•It is this principle, that is central to analysis of personal jurisdiction over the Internet.

Jurisdiction Over Activities on the Internet

•ESAB Group, Inc. v. Centricut, L.L.C.

•Judge Currie in Florence, January 1999

•D filed motion to dismiss for lack of personal jurisdiction

•P DE Corp. ppb Florence, SC developed, manufactured and sold welding systems, including 1 patented electrode

•D NH Corp. manufactured and sold replacement welding parts

•P alleged patent infringement

-Never registered to do business in SC

-Never paid SC taxes

-No employees located in or reside in SC

•P argued sales to SC residents + website = general in personam jurisdiction

Jurisdiction Over Activities on the Internet

•ESAB Group, Inc. v. Centricut, L.L.C.

•Website Analysis within General Jurisdictional Framework

•Court applied the Zippo analysis and found D's Website to be in the middle ground.

-Clearly serves as form of advertisement

-Literature and sample request form

-Provides on-line ordering form

-BUT transaction cannot be completed over the Internet until customer calls toll free number to establish account

-Thus, interactivity of website limited to customers who set up account in advance

•The court went on to reject the notion that jurisdiction could be found based on the fact that the Web page is accessible in the forum. To hold otherwise would be to subject defendants "to jurisdiction on a worldwide basis and would eviscerate personal jurisdiction requirements as they currently exist."

•The court found that merely categorizing a Web site as interactive or passive is not conclusive of the jurisdictional issue. General in personam jurisdiction must be based on more than a defendant's mere presence on the Internet, even if it is an "interactive" presence. Rather the critical issue for the court to analyze is the nature and quality of

commercial activity actually conducted by an entity over the Internet in the forum state, i.e. the Zippo principle.

Jurisdiction Over Activities on the Internet

•ESAB Group, Inc. v. Centricut, L.L.C.

•Website Analysis within General Jurisdictional Framework

•The court then discussed several factors that would impact the "nature and quality" jurisdictional analysis. They can be broken down into five factors:

–1) Commercial activity conducted through the Internet site in South Carolina;

–2) Evidence of South Carolina residence visiting defendant's Web page;

–3) Evidence of South Carolina residents purchasing products based on Web site advertising;

–4) Encouraging South Carolina residents to visit the Web site; and

–5) Directing the Web site at South Carolina residents over residents of other states.

•Each of these weighed in favor of the defendant. The court then noted that in each case cited by the plaintiff to support jurisdiction, the court found "'something more' than defendant's mere presence on the Internet 'to indicate that the defendant purposefully (albeit electronically) directed his activity in a substantial way to the forum state."

•D's website does not constitute a substantial contact with SC for purposes of general jurisdiction.

Jurisdiction Over Activities on the Internet

•ESAB Group, Inc. v. Centricut, L.L.C.

•Specific Jurisdictional Analysis

–Requires D engage in some activity purposely aimed toward SC

-Some cause of action arose directly from that activity

•Sale of Infringing Product to SC Customer

-Generally allows personal jurisdiction

-BUT sale post-dated accrual of the cause of action and appears to be manufactured by P for preferred forum

-1 sale in SC does not satisfy minimum contacts requirement of due process analysis

•Maintenance of D's Website as "Offer to Sell" pursuant to 35 USC § 271(a)

-No allegations any SC residents accessed D's website

-Without some other substantial act, website is not an offer to sell

-Minimum contacts requirements of Due Process Clause are not met

Jurisdiction Over Activities on the Internet

•Brown v. Geha-Werke GmbH

•Judge Norton in Charleston, September 1999

•D filed Motion to Dismiss for Lack of Personal Jurisdiction

•Products liability case involving a paper shredder

•D a German Corp. manufactured the paper shredder

•Traditional SC Contacts for D

-Transacts no business in SC

-No agents or employees in SC

-No agents ever visited SC

-Owns no property in SC

-Does not advertise in SC

-Not licensed to do business in SC

–Does not hold itself out as doing business in SC

–Has not tried to develop market or solicit customers in SC

–Does not provide any services or advice to customers in SC

–Maintains no customer relations network for customers in SC

Jurisdiction Over Activities on the Internet

●Brown v. Geha-Werke GmbH

●Specific Jurisdictional Analysis

●SC Long-Arm Statute

–Found D "barely fits" within subsection (H) of long arm statute

–D had reasonable expectation its high security shredders would be used in SC which had a disproportionately high number of military installations

–Thus, Court may exercise personal jurisdiction over D under long arm statute.

●Due Process Analysis

–Minimum Contacts Analysis

●Court did not buy claim that D designed and manufactured shredders for military use and this is functionally equivalent to designing a shredder for the SC market due to disproportionate number in SC

●D never serviced customers in SC

●D never proven to be driving force behind marketing strategy focusing on SC

Jurisdiction Over Activities on the Internet

●Brown v. Geha-Werke GmbH

●Specific Jurisdictional Analysis

●Court did not find that D had advertised in SC

-P claimed D's Website advertised its product and provided its Internet e-mail address

-Cited to Zippo and its sliding scale analysis and found that defendant's Web site fell into the "passive" Web site category

-Referring to ESAB, the court noted that "merely categorizing a Web site as interactive or passive is not conclusive of the jurisdictional issue"

-Thus, the court applied the five "nature and quality" factors laid out in ESAB and found each of them in the defendant's favor

- Commercial activity in SC
- SC residence visiting
- SC residents purchasing
- Encouraging SC residents to visit
- Directing at SC residents
- Thus, Jurisdiction was not proper under a "minimum contacts" analysis

-Reasonableness Factors

- Due to complete paucity of minimum contacts, the reasonableness factors of the second prong of the Due Process analysis cannot assist P in establishing personal jurisdiction

Jurisdiction Over Activities on the Internet

- Brown v. Geha-Werke GmbH
- General Jurisdiction Analysis

-None of the other factors found in S.C. Code § 36-2-802 applied

-Even if found D were "doing business" in SC, D's complete lack of contacts with SC precludes finding it had "continuous and systematic" contacts with SC

-Thus, asserting general in personam jurisdiction would violate Due Process Clause

●Conclusion

–Insufficient evidence that D purposefully directed any activities toward SC

–Insufficient evidence that D had "continuous and systematic" contacts with SC

–Thus, insufficient evidence to support specific or general jurisdiction over D

Jurisdiction Over Activities on the Internet

●Vinten v. Jeantot Marine Alliances, S.A

●Judge Norton in Charleston, March 2002

●Motion to set aside default judgment and complaint dismissed for lack of personal jurisdiction

●D was French business entity which purchased entity that manufactured catamaran

●P resident of Australia sought damages for an accident involving the catamaran that occurred in Charleston, SC

●P did not present any evidence that D had any contacts with SC

●P argued that website + national advertisement provides necessary minimal contacts for personal jurisdiction

Jurisdiction Over Activities on the Internet

●Vinten v. Jeantot Marine Alliances, S.A

●Website Analysis

–P argued website constituted sufficient contacts with SC for personal jurisdiction

–Noted 4th Circuit has not addressed when a website can satisfy minimum contacts required for personal jurisdiction

–Cited Zippo sliding scale

–Cited Brown, regardless of a website's passivity or interactivity, the essential question remains the same—did D purposefully direct activity at SC

–Cited ESAB, general in personam jurisdiction must be based on more than a D's mere presence on the Internet even if it is Interactive

–Cited Zippo principal: "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet."

Jurisdiction Over Activities on the Internet

●Vinten v. Jeantot Marine Alliances, S.A

●Website Analysis

–Noted that many courts have found that an interactive Web site alone will not establish minimum contacts for personal jurisdiction

–D's website has some degree of interactivity

•provided a form for users to fill out to request additional information

•an e-mail link

–Applied the five factors established in ESAB and found each factor in favor of the defendant

•Commercial activity in SC

•SC residence visiting

•SC residents purchasing

•Encouraging SC residents to visit

•Directing at SC residents

–Website failed to provide the minimum contacts necessary for finding personal jurisdiction

Jurisdiction Over Activities on the Internet

●ALS Scan, Inc. v. Digital Service Consultants

●4th Circuit, June 2002

●Court affirmed District Court's Order dismissing the Claim against D ISP for lack of personal jurisdiction

●Issue: Whether a person electronically transmitting or enabling the transmission of information via the Internet to MD, causing injury thereby, subjects the person to the jurisdiction of a MD court

●P MD Corp. creates and markets adult photographs of female models for distribution over the Internet, brought copyright infringement action

●D GA ISP allegedly enabled co-D to publish P's copyrighted pictures by providing bandwidth service needed to maintain its website

Jurisdiction Over Activities on the Internet

●ALS Scan, Inc. v. Digital Service Consultants

●Specific Jurisdictional Analysis

●Until the due process concepts of personal jurisdiction are reconceived and rearticulated by the Supreme Court in light of advances in technology, we must develop, under existing principles, the more limited circumstances when it can be deemed that an out-of-state citizen, through electronic contacts, has conceptually 'entered' the State via the Internet for jurisdictional purposes.

●Drawing on the requirements for specific jurisdiction, requiring purposeful conduct, the Zippo model is adopted

●State the guiding principle regarding "nature and quality" of commercial activity conducted over the Internet

Jurisdiction Over Activities on the Internet

●ALS Scan, Inc. v. Digital Service Consultants

●Specific Jurisdictional Analysis

●Laid out a three part test to analyze when a State may exercise judicial power over a person outside the State

-1) Directs electronic activity into the State,

-2) With the manifested intent of engaging in business or other interactions within the State, and

-3) That activity creates, in a person within the State, a potential cause of action cognizable in the State's courts.

●The court then explicitly stated that "passively" placing information on the Internet does not subject one to jurisdiction in each State into which the electronic signal is transmitted and received because

-There is generally no electronic activity directed into the State

-With the manifested intent of engaging businesses or other interactions in the State

-That would create a potential cause of action in a person within the State.

●The first 2 factors were held to be in favor of D

●More facts would have to be developed regarding whether D continued to enable the website after receiving notice

•Thus the minimum contacts were not present to assert specific jurisdiction.

Jurisdiction Over Activities on the Internet

•ALS Scan, Inc. v. Digital Service Consultants

•General Jurisdictional Analysis

•Even in the absence of specific jurisdiction, general jurisdiction may exist when D has sufficient contacts with forum

•The court noted that the minimum contacts required for general jurisdiction are significantly higher than for specific jurisdiction and may be asserted when D's activities have been continuous and systematic

•"We are not prepared at this time to recognize that a State may obtain general jurisdiction over out-of-state persons who regularly and systematically transmit electronic signals into the State via the Internet based solely on those transmissions. Something more would have to be demonstrated. And we need not decide today what that "something more" is… because ALS has shown no more."

•D has engaged in no activity in MD other than maintain its website on the Internet and its only contacts with MD occur when MD persons access D's website

•The court went on to state that while electronic transmissions from maintenance of a Web site may result in numerous and repeated electronic connections with persons in a state, these transmissions do not constitute the quality of contacts necessary for a State to have general jurisdiction.

•Based on the foregoing analysis of both specific and general jurisdiction, the court held that the Georgia based ISP did not subject itself to personal jurisdiction in Maryland by

enabling a Web site owner to publish photographs over the Internet in violation of a Maryland corporation's copyrights.

Jurisdiction Over Activities on the Internet

●Website Interactivity Analysis

–"Passive" Web sites in which the defendant has done nothing but advertise its product on the Internet. Most courts find personal jurisdiction cannot be exercised in these cases.

–"Interactive" Web sites whereby individuals enter into contracts with defendants via the Internet and download, transmit or exchange files. As is expected, courts have found personal jurisdiction proper in these cases.

–In between these two categories are Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.

●Zippo Principle

–The "likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet."

Jurisdiction Over Activities on the Internet

●SC factors that impact the "nature and quality" jurisdictional analysis

–1) Commercial activity conducted through the Internet site in South Carolina;

–2) Evidence of South Carolina residence visiting defendant's Web page;

–3) Evidence of South Carolina residents purchasing products based on Web site advertising;

–4) Encouraging South Carolina residents to visit the Web site; and

–5) Directing the Web site at South Carolina residents over residents of other states.

●4th Circuit factors impacting the "nature and quality" jurisdictional analysis

–1) Directs electronic activity into the State,

–2) With the manifested intent of engaging in business or other interactions within the State, and

–3) That activity creates, in a person within the State, a potential cause of action cognizable in the State's courts.

PowerPoint Presentation Regarding Intellectual Property Issues on the Internet

Intellectual Property Issues on the Internet

Wade M. Chumney, Esq.

Intellectual Property

●Rationale: to stimulate creativity without unduly displacing the benefits that normally flow from free competition

●Tension

●Congress has increased IP Protection

–American Inventors Protection Act

–AntiCybersquatting Consumer Protection Act

–Sonny Bono

–Digital Millennium Copyright Act

–Economic Espionage Act 1996

●4 Foundations

–TM

–CR

–Patent

–TS

Trademarks

●Primary purpose not to stimulate creative energies (like CR, Patent, and TS) but to:

–Combat unethical marketing practices

–Protect goodwill

–Enhance the efficient distribution of goods and services

–Provide consumers shorthand way for finding goods or services they desire

Trademarks

●Protects a word, name, symbol, or device used to identify the source of a good and distinguish it from the products of another

●Mark must be distinctive, meaning it must be capable of identifying the source of a particular good

–Mark may be protectable if it has acquired a secondary meaning

●Four categories based upon the relationship between the mark and the underlying product:

–1) Arbitrary or Fanciful

●Bears no logical relationship to the underlying product

–2) Suggestive

●Suggests a characteristic of the underlying good

–3) Descriptive

●Directly describes a characteristic of the underlying product

–4) Generic

●Describes the general category to which the underlying product belongs

–To prove trademark violation, the plaintiff must show that there was a

●Protectable mark

●Likelihood of confusion

Trademark Dilution

●FTDA in 1996

●"Lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of:

-1) Competition between the owner of the famous mark and other parties

-2) Likelihood of confusion, mistake or deception.

●Famous factors

-Distinctiveness

-Duration and extent of use

-Duration and extent of advertising and publicity

-Geographical extent

-Channels of trade

-Degree of recognition of the marks

-Nature and extent of use by third parties

-Federally registered

●Implications of FTDA

-Protects famous marks regardless of a showing of competition or likelihood of confusion

-Owners of famous marks can argue almost every conceivable commercial use of their marks may whittle away their distinctiveness or tarnish their image

Copyrights

●Copyright law governs the right to control copying of certain works

●To qualify for copyright protection, the work must be an original work of authorship fixed in a tangible medium of expression

●Copyright protection is available only for the expression of an idea, i.e. the "work", and does not extend to the idea itself or any procedure, process, system, method of operation, concept, principle, or discovery

●Copyright protection exists automatically once the work is fixed in a tangible medium of expression

●Copyright protection for works created after January 1, 1978, lasts for 70 years after the author's death

Copyrights

●Internet causes substantial change in way works may be copied, decreasing cost and increasing quality

●Copyright monopoly is as much about distribution as creation

●So time is near when CR wont be meaningful in terms of ensuring distribution—Copyrights will be predominantly about content

●Competing Views

–Copyright needs to be strengthened

–Copyright losing importance

Copyrights

●Copyrights and Software

●Judicial Limitations

●Clean-room techniques

–Two rooms one takes program and produces flow charts (dirty room: ideas and expression goes in, only ideas come out);

–Other takes flow charts and writes program (original ideas new expression).

●Computer companies now look more to patents and trade secrets

The Digital Millennium Copyright Act

●DMCA enacted on October 27, 1998, affected the liability of individuals who use copyrighted works on the Internet.

–Limits Internet Service Providers (ISPs) liability

●Safe Harbor re: removal of Copyrighted Works

●Caching

–Protects against anti-circumvention technologies by providing civil remedies for two related acts

●Circumventing prohibited

●Trafficking prohibited

●Too much control?

The Digital Millennium Copyright Act

●ALS Scan v. Remarq Communications

–The defendant ISP gave its subscribers 30,000 newsgroups in which they could participate. The plaintiff sent defendant a letter of objection demanding plaintiff stop carrying two newsgroups which had ALS's name in their titles and allegedly displayed thousands of ALS's copyrighted photographs.

–DMCA was enacted to both preserve copyright enforcement on the Internet and to provide immunity to ISPs from copyright infringement liability for "passive" "automatic" actions in which an ISP's system engages without the knowledge of the service provider.

–Immunity is lost if an ISP:

•1) Has actual knowledge of the infringement or is aware of facts or circumstances from which the infringing activity is apparent

•2) Receives a financial benefit directly attributable to the infringing activity and has a right and ability to control it

•3) Receives notice of the claimed infringement and fails to remove or disable the material

–The court found for the plaintiff based on the third factor

Metatags

●A metatag is hypertext markup language ("HTML") code that permits Web designers to describe their Web page

–The keyword metatag permits designers to identify search terms for use by search engines

–Description metatags allow designers to briefly describe the contents of their web pages

●Keyword metatags should contain keywords relating to the contents of the web site

–More likely it is that the web page will be 'hit' in a search for that keyword

–Higher on the list of 'hits' the web page will appear

●Three common situations

–1) Rival

–2) Free speech

–3) Increase hits w/o rational relationship

●Valuable because advertising rates based on # of hits

●The unauthorized use of a TM in a metatag

–Intentional use of a TM to sell or promote alternative goods or services

–Clear example of consumer confusion

Metatags

• Playboy Enterprises, Inc. v. Welles

–Terri Welles, Playboy Playmate of the Year in 1981, was sued for trademark infringement based in part on her use of the terms "Playboy" and "Playmate" in her site's metatags

–Court found that the defendant's use of the terms in metatags constituted permissible, nominative use as:

•1) There was no descriptive substitute for the two terms

•2) To preclude the use of metatags would have the undesirable effect of hindering the free flow of information on the Internet

–But Court indicated its decision might be different if the metatags listed the trademark term so repeatedly that Welles' site regularly appeared above the plaintiff's in results obtained when "playboy" or "playmate" were entered in a search engine.

Metatags

•Bihari v. Gross

–Defendant used plaintiff's marks in metatags to defendant's site that criticized the plaintiff's interior decorating service

–The use was found not likely to cause confusion and a protected fair use that described the contents of the Web site

–Court noted that to hold otherwise and prohibit use of plaintiff's mark in metatags of all sites not authorized by plaintiff would effectively foreclose all comment about the plaintiff

Metatags

●Bernia of America, Inc. v. Fashion Fabrics International

–Defendant owned a site that misleadingly portrayed it as an authorized dealer of the plaintiff

–The court enjoined the defendant from using plaintiff's marks within its metatags

–The court noted; however, that if the defendant had merely been reselling plaintiff's goods without the use of misleading representations, use of the plaintiffs' marks in metatags would have been proper

Hyperlinking

●Cross-reference appearing on one Web page that, when activated, brings up another Web page

–Text, such as the Internet address ("URL") of the web page being called up

–Word or phrase that identifies the web page being called up

–Image

●The code for the web page containing the hyperlink contains a computer instruction that associates the link with the URL of the web page to be accessed so that clicking on the hyperlink instructs the computer to enter the URL of the desired web page and thereby access the page

●Tremendous benefit to the user, allowing for efficient access to desired information

Hyperlinking

●Trade Tent Analogy

●Copyright Issues

–Top level Web page

●Little likelihood of confusion exists

–"Deep hyperlink"

●more likely to cause confusion

●Linking does not raise copyright issues generally

–Implied consent

–Fair use

●Trademark Issues

–Ok if links to proper source

–If have porno ads then could argue tarnishment

–Embedded pages (deep hyperlinks)

–Ticketmaster v. Microsoft

●Link to a site you reasonably know has unauthorized work

–Contributory infringement

Hyperlinking

●Ford Motor Co. v. 2600 Enterprises

–Defendant registered the domain name fuckgeneralmotors.com and visitors who entered the site were automatically linked to Ford's home page

–The plaintiff sued claiming the use of "ford" in defendant's programming code to create a hyperlink to Ford's homepage constituted trademark dilution and infringement

–In finding for the defendant, the court indicated that the dilution act was not intended to be a tool for eliminating all Internet links that, in the subjective view of the trademark holder, somehow disparage its trademark

–The court went on to state that trademark law does not permit a party to enjoin others from linking to its home page simply because it does not like the domain name or content of the linking Web page

Hyperlinking

●Kelly v. Arriba Soft Corp.

–Defendant operated a search engine that allowed a user to type in search terms and receive results in the form of "thumbnails," small picture versions of full sized pictures contained at other Web sites. When the plaintiff discovered his photographs had been included in the search engine database, he filed suit for copyright infringement

–The court held that the creation and use of the thumbnails was fair use because it was a transformative use of improving access to information on the Internet

–The court determined that due to the low resolution used in creating the thumbnails and the degradation in the image if enlarged, it was extremely unlikely that anyone would enlarge the thumbnail and use it for illustrative or aesthetic purposes

Framing

●Allows Internet users to view contents on one site while remaining on the initial page

●The second window appears on the screen framed by the first site

●Greater concern than linking

–Sections Viewed

–URL

Framing

●Copyright

–If entire page is framed

●Infringement

●No fair use because negative effect on advertising revenues

–Derivative work if size diminished

–Implied consent

–Fair use

●Trademark

–Tarnishment argument

Framing

●Kelly v. Arriba Soft Corp.

–Court dealt with the issue of framing in addition to hyperlinking

–Found for the plaintiff with respect to the importation of pictures from the originating Web site and the display of the larger image within the frame of defendant's Web site. The court referred to this practice as inline linking, defining it as:

–"[t]he process of importing an image from another web site…The image imported from another web site is displayed as though it is part of the current Web page, surrounded by the current Web page's text and advertising. As a result…the user [may] not realize that the image actually resided on another web site."

–Finding no fair use, the court held that defendant's importation of plaintiff's work violated plaintiff's exclusive right to publicly display his works

–The use was not transformative use to access information on the Internet, but was rather the end product itself and it substituted for users accessing the full images on plaintiff's site

Content Rights Issues

●Refers to the general appearance and style of a Web site, trade dress law appears applicable

●While trade dress was originally intended to protect a product's packaging, protection has been extended to include the total appearance of a product, including its size, shape, color, texture, and graphics

●To prove infringement, one must show likelihood of confusion and that the trade dress is both distinctive and nonfunctional

Content Rights Issues

●Tensions with design patents

–When product designs not protected by design patent, supposed to be freely available for competitors

●Limited exception allowing TM protection when necessary to protect consumers from confusion and under circumstances that will not yield competitive barriers

●More complex than name and word analysis because features may be intimately connected to functioning products

●Issue is whether software has sufficiently unique characteristics to allow customers to distinguish it and whether those attributes are somehow superior for the ways customers use the product

●Concerns if becomes standard in the industry

Content Rights Issues

●Playboy Enterprises, Inc. v. Calvin Designer Label

–The court enjoined the defendant from "disseminating, using, or distributing any Website pages whose appearance so resembles the Website pages or trademarks used by [Playboy] so as to likely create a likelihood of confusion, mistake or deception"

●Computer Care v. Service Systems Enterprises

–Found trade dress infringement based upon the defendant's copying of the layout of plaintiff's computer-generated sale brochure, reminder letters and monthly reports

Domain Name Issues

●Value of Domain Name

●One should not invest good will into a domain name without assurance domain name will stand up in court if challenged

●Decision of domain name registrar carries no special weight at this time, may change if domain name registration policies become more integrated with TM laws in the future

Domain Name Issues

●Congress passed the Anticybersquatting Consumer Protection Act (ACPA) in 1999 to address domain name issues.

–"to protect consumers and business…and to provide clarity in law for trademark owners by prohibiting the bad-faith…registration of distinctive marks as Internet domain names with the intent to profit from the goodwill associated with such marks…"

–In addition to prohibiting registration of domain names in bad faith, the Act also precludes dilutive registrations and enables courts to cancel or transfer domain name registrations and/or impose civil penalties against offenders.

–Gives 9 "bad faith" factors

–Statutory damages from $1,000 to $100,000 per domain name

Domain Name Issues

●ICANN

–UDRP Pursuant to the UDRP, the domain name holder must submit to a mandatory arbitration proceeding should a third party complainant bring a proceeding regarding the domain name

–Three part requirement for the complainant to prevail:

•1) Domain name is identical or confusingly similar

•2) Holder has no rights or legitimate interests

•3) Bad faith

●Either may submit the dispute to a court prior to commencement

●During a UDRP proceeding, a domain name dispute cannot be cancelled, transferred, activated, or deactivated until a decision is rendered

●Remedies

–Cancellation of the domain name registration

–Transfer of the domain name to the complainant

–Losing party has 10 days to commence a lawsuit

Domain Name Issues

●Suck sites

–Global soapbox with virtually unlimited audience

●Examples:

–Aolsucks.org

–Microsoftsucks.org

–Cokesucks.com

–Nikesucks.com

●Bally Total Fitness

–TM with sucks across not commercial because only expressed view

–Not tarnished because only unflattering commentary

●Solution

–Could purchase all derivations of co. name, but expensive and may miss

●Verizon

Domain Name Issues

●Solutions for Domain Name Disputes

–Increase number of registrars

–Increase number of TLDs

●Might cause greater consumer confusion

–Greater reliance on country-based TLDs

●But .com has international scope

–Directory systems

●Ex: apple.com leads to apple computer, apple records and others and you choose with hyperlinks

Domain Name Issues

●People for the Ethical Treatment of Animals v. Doughney

–People for the Ethical Treatment of Animals sued defendant after he registered the domain name peta.org and organized a Web site called People Eating Tasty Animals, complete with links to fur and meat sites

–The defendant argued unsuccessfully that the domain name should be considered in conjunction with its Web site, which parodies plaintiff's site. The court determined that consumers encounter defendant's domain name alone without the site's content, and thus no parody defense could be established.

–The court found that the defendant violated the ACPA and acted in bad faith because he: 1) had no intellectual property rights in peta.org; 2) used PETA in a commercial manner; 3) intentionally diverted Internet users from plaintiff's site; 4) made statements to the press suggesting PETA buy the site from him; 5) made false statements in registering the domain name; and 6) registered other domain names incorporating other's names or marks.

Domain Name Issues

●Vivendi Universal v. Sallen

–UDRP decision, complainant filed a complaint against Sallen who registered the domain name vivendiuniversalsucks.com

–Panel found the disputed domain name confusingly similar despite acknowledging that there is an "unresolved disagreement between panels…as to whether a <[trademark]sucks.com> domain name can ever be confusingly similar to the trademark to which the word sucks is appended."

–Finding the respondent had no interests in the disputed domain name, the Panel rejected his free speech argument because the respondent made no use of the domain name until he received a "cease and desist" letter

–Relying on respondent's prior knowledge of Vivendi's mark and passive holding of the domain name, the Panel found that he registered the mark in bad faith and required the domain name be transferred to Vivendi

Patents

●A patent is a right granted by the federal government to an inventor enabling him to exclude others from making, using, selling, or importing the invention within the US without the inventor's consent

●Patents are filed with the PTO and generally last for a term of 20 years from the date of filing

●For an invention to receive patent protection it must be:

–1) new,

–2) useful, and

–3) non-obvious

Patents

●State Street Bank & Trust Co. v. Signature Financial Group

–patent on a computer system valid because it demonstrated a method of operation on a computer to effectuate a business activity

●Examples of Internet Patents issued by PTO:

–System to carry out reverse sellers' auctions over the Web (Priceline.com, Inc.)

–One-click ordering system that stores a customer's billing and shipping information does not have to be reentered on subsequent visits (Amazon.com)

–A patent for on on-line frequent buyers program that rewards Web shoppers with benefits such as American AAdvantage Miles (Netincentives, Inc.)

-A patent for a method for delivering advertising on the Internet (DoubleClick, Inc.)

-A patent related to the "shopping cars" which are used to aid on-line purchasing (Open Market, Inc.)

-A system that pays computer users for responding to on-line advertisements and surveys (Cybergold)

-A method that permits customers to choose options for a car ordered over the Internet (Trilogy Software, Inc.)

-System to embed Web addresses in e-mail postings (Thomas Higley)

Patents

● Internet Patents

—Ability to stifle e-commerce

—Compton's New Media Patent in 1993

—PTO overlooks relevant prior art

—PTO's grant is only a presumption of validity

● May present evidence not found or reviewed by PTO

Patents

● Amazon.com, Inc. v. Barnesandnoble.com

-Obtained a patent for the "one-click" shopping process it employs at its site. Claimed that the "one-click" technology, that allowed consumers to shop at its Web site without having to re-enter shipping and billing data for each independent purchase made at the site, was being copied by Barnesandnoble.com

-Amazon.com requested the court order an injunction against Barnesandnoble.com, and an award of monetary damages

–The circuit court did file a preliminary injunction against barnesandnoble.com

–Court of Appeals for the Federal Circuit vacated the preliminary injunction and remanded the case. The court stated that while Amazon.com carried its burden on the likelihood of success on infringement, Barnesandnoble.com raised several questions concerning the validity of the patent.

–This suit settled in March of 2002 with undisclosed terms

Trade Secrets

●Trade secrets protect valuable assets for potentially infinite period of time.

●With emergence of computer technologies, electronic mail, and the Internet value of assets placed in jeopardy

●Pursuant to South Carolina's Trade Secret Act, a trade secret is:

–1) Information including, but not limited to, a formula, pattern, compilation, program, device, method, technique, product, system, or process, design, prototype, procedure, or code that:

–2) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by the public or any other person who can obtain economic value from its disclosure or use and

–3) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Trade Secrets

●Economic Espionage Act 1996

–Crime to steal trade secrets in Interstate commerce or foreign commerce

–Tailored after UTSA

–Defines trade secret broadly as "all forms and types of financial, business, scientific, technical, economic, or engineering information"

–Like UTSA, information must derive its value from fact that

•It is not known or readily ascertainable by public and

•Must be subject to reasonable security measures

–Recognizes info may be stored in various electronic forms

–Activities constituting trade secret theft include: uploading, downloading, transmitting, and replicating

–Individuals convicted can be imprisoned up to 10 years and fined $500,000

–Corporations fined up to $5 million

–Those found guilty of trade secret theft may be required to forfeit not only the proceeds derived from the misappropriation but also the facilities or property used to carry out the crime

Trade Secrets

•Religious Tech. Ctr. v. Lerma

–Washington Post published an article containing information from documents that the plaintiff claimed to be trade secrets. The Washington Post obtained the documents from unsealed court files; additionally, the information contained in the documents was available on the Internet.

–The court denied the Church's request for injunctive relief, due partly to public domain concerns. The court held that once information is posted on the Internet, the information loses its trade secret status.

–"Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely down loads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet."

Trade Secrets

●Trade Secret Protection Measures

–Use employee confidentiality agreements

–Specifically inform employees of trade secrets

–Physically restrict access to trade secrets

–Maintain computer system security

●Access restrictions (passwords, bioware)

●Input phony code into data so copying can be easily proven

●Limit distribution of source code

●Scramble data transmissions

●Restrict software use to hardware within secure areas

–Completely destroy written information

–Do not provide access to entire trade secret

–Screen repair and service personnel

–Restrict plant tours

–Screen speeches, publications, and trade show materials

–Conduct employee exit interviews

–Deal with third parties appropriately

–Make covenants not to compete

PowerPoint Presentation Regarding Defamation, Right of Publicity and Privacy of the Internet

Defamation, Right of Publicity Law and Privacy of the Internet

Wade M. Chumney, Esq.

Defamation, Right of Publicity Law and Privacy of the Internet

- Changes in Technology
- Increasing Speed of Changes
- Communications
- Far Reach of Even Simple Messages
- Anonymity of Communications

Defamation, Right of Publicity Law and Privacy of the Internet

- Implications of Changes
  - Potential for Impact
  - Far Reaching Scope
  - Lag of Law Development

DEFAMATION

DEFAMATION

- Recognizes Value in Reputation
- Recovery for Injury to Reputation
- Resulting From False Communications

DEFAMATION

● Interplay of Constitution

● Not for Mere Hurt Feelings

● "[T]here is a great deal of the law of defamation which makes no sense."

–W. Page Keeton, *et al., Prosser and Keeton on the Law of Torts*, §111, at 771 (5th ed. 1984)

DEFAMATION

Elements:

•Making of a Statement That Is Both

•False, and

•Defamatory

•Statement Is

•Unprivileged, and

•Published to a Third Party

DEFAMATION

Elements:

•Statement Publisher at Fault

And

•Either:

•Statement Actionable Irrespective of Harm, or

•Publication Caused Special Harm

DEFAMATION

Categories:

•Liable

•Slander

DEFAMATION

Slander:

•Verbal statements

DEFAMATION

Liable:

•Everything else

●Written Statements

●Non-verbal Communications

DEFAMATION

Liable or Slander: WHO CARES?

●Different Elements of Proof

DEFAMATION

●Defamation *Per Se*

●Defamation *Per Quod*

DEFAMATION

●Defamation *Per Se*

—Defamatory Meaning Clear From the Face of the Defamation

—Defamation Is a Question of Law

DEFAMATION

●Defamation *Per Quod*

–Requires:

●Reference to or Understanding of

●Facts or Circumstances

●Extrinsic to the Face of the Defamatory Statement

–Any Innocent Construction or Ambiguity

–Jury Question

DEFAMATION

●Actionable *Per Se*

—Also Called "Defamation *Per Se*"

—Pleading/Proof Distinction

DEFAMATION

Actionable *Per Se*

●Pleading/proof Distinction

—Presumption of Common Law Malice

●UNLESS Privileged—then Must Prove

—Presumption General Damages

DEFAMATION

NOT Actionable *Per Se*

● Pleading/Proof Distinction: Plaintiff Must Plead and Prove:

—Common Law Malice

—Special Damages

DEFAMATION

Liable or Slander: WHO CARES?

● Different Elements of Proof to Establish Actionable *Per Se* Defamation

DEFAMATION

Actionable *Per Se:* SLANDER

● Slanderous Statement Must Impute:

—Commission of a Crime of Moral Turpitude

—Contraction of a Loathsome Disease

DEFAMATION

Actionable *Per Se:* SLANDER

● Slanderous Statement Must Impute:

—Adultery

—Unchastity

—Unfitness in One's Business or Profession

DEFAMATION

Actionable *Per Se:* Liable

● Libelous Statement:

—Written or Printed Words

●Tend to Degrade a Person or

●Reduce Character or Reputation Among Friends or Acquaintances, or the Public or

DEFAMATION

Actionable *Per Se:* Liable

●Libelous Statement:

—Written or Printed Words

●Disgrace the Person, or

●Render the Person Odious, Contemptible, or Ridiculous

DEFAMATION

Actionable *Per Se:* Liable

●Reality:

Libelous Statement Always

(Almost) Actionable *Per Se*

DEFAMATION

Privilege

●*Absolute Privilege*

●*Qualified Privilege*

DEFAMATION

Absolute Privilege

●Acts of State

—Judicial Proceedings

—Legislative Proceedings

—Where Publishing Particular Materials Is Required by Law

DEFAMATION

Qualified Privilege

●Occasion Qualifies for the Privilege

●Privilege Is Not Abused

DEFAMATION

Qualified Privilege

●Occasion Qualifies for the Privilege

–Question of Law

–Nature of Communication

●Publisher Has Interest in the Subject Matter

●Recipient Has Similar Interest

●Communication Honestly Made to Protect Common Interest

DEFAMATION

Qualified Privilege

●Privilege Is Not Abused

–Question of Fact

–Weigh Factors

●Good Faith

●Scope of Statement Properly Limited

● Published Only to Appropriate Parties

DEFAMATION

Qualified Privilege

●Officers and Employees

●Promotion or Protection of

–Law Enforcement Interests

–Common Business Interests

–Religious Interests

●Good Faith and in the Normal Course of Business

DEFAMATION

Malice:

●Private v. Public Figure

–Different Standards

–Different Proof

–Different Analysis

DEFAMATION

Malice: Private Plaintiff

●NOT Constitutional Malice

●Common Law Actual Malice

–Defendant Either Acted With

●Ill Will

●Recklessly

●Wantonly

DEFAMATION

Malice: Private Plaintiff

●Common Law Actual Malice

—Defendant Acted With

●Conscious Indifference Toward Plaintiff's Rights

DEFAMATION

Malice: Private Plaintiff

●Common Law Actual Malice

—Belief in Truth Irrelevant

—Published in Manner:

●Improper, or

●Unjustified

DEFAMATION

Malice: Private Plaintiff

●Common Law Actual Malice

—Jury Question

DEFAMATION

Malice: Public Plaintiff

●Constitutional Actual Malice

—Knowledge of False Statement, or

—Reckless Disregard for Statement's Truth

—Mere Ill Will Insufficient

—Common Law Malice Insufficient

RIGHT OF PUBLICITY

AND PRIVACY

Right Of Publicity

And Privacy

●Right of Publicity Recognizes Economic Value in Person's Identity

—Compensation Issue

—Welcome Publicity or Seek to Avoid It

●Right of Privacy

—Preserve Desire to Be Left Alone

—Circumstances Violation of Such Desire Is Actionable

Right Of Publicity

And Privacy

●1890 Warren and Brandeis Law Review Article

●Called for Extension of Existing Common Law Privacy Rights

●Goal=protect Individuals From:

Right Of Publicity

And Privacy

"[T]he Advancing Threat of a Society Overrun With Technology and Consumed With Gossip"

Right Of Publicity

And Privacy

●Prosser Developed 4 Categories

●Late Adopted in Restatement:

—Intrusion Upon Plaintiff's Physical Solitude

—Public Disclosure of Embarrassing Private Facts

Right Of Publicity

And Privacy

● Prosser Developed 4 Categories

—False Light in the Public Eye, and

—Appropriation of Plaintiff's Name or Likeness for Commercial Benefit

Right Of Publicity

And Privacy

● South Carolina Version:

—Unwarranted Appropriation or Exploitation of One's Personality

—Publicizing One's Private Affairs With Which the Public Has No Legitimate Concern,

or

Right Of Publicity

And Privacy

● South Carolina Version:

—Wrongful Intrusion Into One's Private Activities, in Such Manner As To:

● Outrage, or

● Cause Mental Suffering, Shame, or Humiliation in

● Person of Ordinary Sensibilities

Right Of Publicity

And Privacy

● South Carolina Version:

—NO "False Light in Public Eye"

—Consistent Approach of State

Right Of Publicity

And Privacy

Most Common in South Carolina:

Publicizing One's Private Affairs With Which the Public Has No Legitimate Concern

Right Of Publicity

And Privacy

● Publicity ≠ Defamation Publication

● Not Means of Communication

● Scope of Audience

—Public v. Private Communication

—Reaches, or Is Sure to Reach, the Public

—Not If to a Single Person or a Small Group

Right Of Publicity

And Privacy

—Any Publication in a Newspaper

—Any in Magazine—regardless of Circulation

—Handbill Distributed to a Large Number

—Any Broadcast Over the Radio

—Statement to a Large Audience

Right Of Publicity

And Privacy

Publicity Component: South Carolina

- Improper Usurpation of a Person's Identity

SPECIAL PROBLEMS ON THE INTERNET

SPECIAL PROBLEMS ON THE INTERNET

- John Doe Lawsuits and Business Defamation
- John Doe Plaintiffs

Special Problems On The Internet

John Doe Lawsuits

- Easy to Post True, Accurate, and Useful Information
- Just As Easy to Post False, Unflattering, Unsubstantiated or Outright Malicious Information

Special Problems On The Internet

John Doe Lawsuits

- Chat Rooms and Bulletin Boards and Damaging Information

—Personal or Business Related

—Ready Avenue for Presentation

—Ready Avenue for Dissemination

SPECIAL PROBLEMS ON THE INTERNET

John Doe Lawsuits

● Purposes of Dissemination

—Manipulate Stock Prices

—Disgruntled or Disloyal Employee

—Seeking to Embarrass or Humiliate

Special Problems On The Internet

John Doe Lawsuits

● Corporate Response to Risk :

Vigilance

Special Problems On The Internet

John Doe Lawsuits

● Vigilance

—In Relation to Sensitivity to Public Image

—Search for Defamatory Postings

—Respond When Discover Postings

Special Problems On The Internet

John Doe Lawsuits

Response:

● Contact ISP

● Demand Removal of Offending Information

● ID Defamer

Special Problems On The Internet

John Doe Lawsuits

Identify Defaming Poster

- Typically Anonymous
- Demand ISP Release Identity

—Yahoo! Used to Respond

—Privacy Concerns on Internet Have Led to Most Isp's Refusing W/o Court Order

Special Problems On The Internet

John Doe Lawsuits

- John Doe Lawsuit—no Name
- Subpoena ID of Poster From ISP
- ISP May Fight to Protect Public Image
- John Doe May Fight to Protect Self

Special Problems On The Internet

John Doe Lawsuits

- Battle of ID

—Privacy

—Free Speech Rights

- Chilling Effect of Loss of Anonymity

—Protection of Reputation

SPECIAL PROBLEMS ON THE INTERNET

Immunomedics, Inc. v. Jean Doe

- Poster Claimed to Be Employee

●Negative Info Posted

—Europe Division Out of Stock

—European Division Manager to Be Fired

●Employment Confidentiality Breach

Special Problems On The Internet

Immunomedics, Inc. v. Jean Doe

●Trial Court Ordered Identification

●Appellate Court Affirmed

Special Problems On The Internet

Immunomedics, Inc. v. Jean Doe

●Balance

— The Necessity of Disclosure

—With the Free Speech Rights of the Anonymous Poster

Special Problems On The Internet

Immunomedics, Inc. v. Jean Doe

—Prima Facie Case Made

—Disclosure Appropriate

Special Problems On The Internet

RIAA v. Verizon

● Recording Industry Association of America Subpoena for Identity Verizon System User

●Verizon Claims Passive Conduit

–No Offending Material Stored on Verizon System

–Subpoena Invalid Under the Digital Millennium Copyright Act

Special Problems On The Internet

AOL v. Nam Tai Electronics

- AOL Largest ISP
- AOL HQ in Virginia
- Virginia's Highest Court
- November 1, 2002

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Nam Tai Sought ID on Stock Messages
- Filed Suit Against 51 John Does in California
- Subpoena to AOL in Virginia
- AOL Moves to Quash

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Nam Tai Sought ID on Stock Messages
- Filed Suit Against 51 John Does in California
- Subpoena to AOL in Virginia
- AOL Moves to Quash

Special Problems On The Internet

AOL *v. Nam Tai Electronics*

- AOL Essentially Seeks Different Free Speech Rule of Law Than Non E-World
- Trial Court Applied Uniform Foreign Depositions Act

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Messages Posted on Yahoo! Board
- Board Devoted to Nam Tai Stock
- Negative Assessment of Stock
- Nam Tai Claimed

–Unfair Trade Practice

–Interfere With Stockholder Relations

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Messages Posted on Yahoo! Board
- Board Devoted to Nam Tai Stock
- Posting Required Yahoo! Account

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Negative Assessment of Stock
- Nam Tai Claimed

–Unfair Trade Practice

–Interfere With Stockholder Relations

Special Problems On The Internet

AOL v. Nam Tai Electronics

●Negative Assessment of Stock

●Nam Tai Claimed

–Unfair Trade Practice

–Interfere With Stockholder Relations

Special Problems On The Internet

AOL v. Nam Tai Electronics

●*AOL* Claims Free Speech Trumps All Counts

●Nam Tai Claims

–Comity on Calif. Court

–Improper to Seek Review of Calif. Decision

Special Problems On The Internet

AOL v. Nam Tai Electronics

●Trial Court Deferred Pending Info Form California Court on Procedural and Substantive Law

●California:

–Complaint Alleges Sufficient Facts for Discovery

–Privacy Outweighed by Right of Calif. Companies to Conduct Out-of-State Discovery

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Trial Court Held No Comity on Defamation Because Allegations Insufficient
- Comity on Unfair Trade Practices
- Discovery Allowed

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Va. Supreme Court Agreed:

—Same 1st Amend. Rights in CA As VA

—Proper for CA Court to Address Issue

- Case No. 012761, 2002 Va. Lexis 157

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Implications

—If Va. Won't Protect AOL, Nobody Will

—Careful Plaintiff Should Be Able to Allege Enough to ID Poster of Commercial Information

—Still Unclear on Other Types of Speech

Special Problems On The Internet

AOL v. Nam Tai Electronics

- Implications

—If Va. Won't Protect AOL, Nobody Will

—Careful Plaintiff Should Be Able to Allege Enough to ID Poster of Commercial Information

–Still Unclear on Other Types of Speech

Special Problems On The Internet

John Doe Plaintiffs

- Attacking Poster Can Correct
- Attacking Poster Draws Attention

Special Problems On The Internet

John Doe Plaintiffs

- *AOL v. Anonymous Publicly Traded Company*

–Defamation

–Former Employee Confidentiality

- Use "Coercive Powers" of the Court System
- Avoid Identifying Self
- AOL Moved to Quash the Subpoenas in Va.

Special Problems On The Internet

John Doe Plaintiffs

- *AOL* Sought Identity of Company
- Indiana Court Granted Motion for Anonymity
- Trial Court Acknowledged 1st Amend. Issue
- Trial Court Denied Motion to Quash

Special Problems On The Internet

John Doe Plaintiffs

●Va. Supreme Court Reversed

—Uncertain Pers. Jur. In Ind. Over Anon. Defendant

—Ind. Anonymity Ruling Made *Ex Parte*

—No Facts or Analysis Form Ind. Court

Special Problems On The Internet

John Doe Plaintiffs

—No Way to Determine If Ind. And Va. Procedural and Substantive Law Were

Reasonably Comparable

—Weighs Against Comity

Special Problems On The Internet

John Doe Plaintiffs

●Privacy of Plaintiff

—Not Absolute Right to Know Plaintiff

—Avoid Annoyance/criticism Attendant to Litigation

—Preserve Privacy of Sensitive/highly Personal Matter

Special Problems On The Internet

John Doe Plaintiffs

●Privacy of Plaintiff

—Risk of Retaliatory Physical or Mental Harm to

●Requesting Party or

●Innocent Non-parties

—Ages of the Persons to Be Protected by Privacy

Special Problems On The Internet

John Doe Plaintiffs

- Privacy of Plaintiff

—What Interest Is to Be Protected

—Action Against a Governmental or Private Party

—Risk of Unfairness to the Opposing Party

Conclusion

- Developing Area of the Law
- Same Standards Likely to Apply in E-world
- More Potential for Harm Out of Less Action
- Careful Complaint Should Get to ID of Posters
- Special Damages/harm More Likely Presumed
- Privacy Issues Discussed Under Ethics Portion

PowerPoint Presentation Regarding Legal Issues in E-Commerce

ELECTRONIC COMMERCE

Wade M. Chumney, Esq.

ELECTRONIC COMMERCE

What Is It?

- First High-Tech for "On-Line Shopping"
- Far Eclipsed That Narrow Concept
- "E-Tailer" Finds:

–Customers

–Competitors

–Suppliers

ELECTRONIC COMMERCE

"E-Tailer" Finds:

–Service Providers (Accountants and Attorneys)

–Government Regulators

- Industrial Users:

–Exchange Information and Data

–Track Raw Materials, Component Parts and Developments in Relevant Markets They Service

ELECTRONIC COMMERCE

- World Wide Parties join together in commerce
- Never seen each other

- Never or met each other
- May not be sure that they are who they say
- E-commerce is a market place.

ELECTRONIC COMMERCE

What Is It?

A Market Place That Utilizes and Leverages the Technologies of the Internet and the World Wide Web, Including Email, Electronic Fund Transfers, Smart Cards, and Electronic Data Exchange and Interchange As Its Backbone

BASIC CONTRACT CONSIDERATIONS

- E-Commerce Raises Unique Issues
- Ongoing Relationship w/ Regular Partners
- Single Transactions
- Lag of Law Behind Technology
- Engaging in business electronically poses a number of unique issues. In some instances, it will be an ongoing relationship between regular trading partners. In other instances there will be no ongoing business relationship with any particular individual or entity. Although the law of cyberspace has made some serious advances, it will likely trail behind technology for years to come.

BASIC CONTRACT CONSIDERATIONS

- Foreign Trading Partners
- Partners Where No Uniform Computer Information Transactions Act or Uniform Electronic Transaction Act
- Address by Contract Concerns Not in the Law

●Multi-level, Multi-function

●Multiple Parties

●Define Own Rules

BASIC CONTRACT CONSIDERATIONS

●Especially for states not having adopted some form of the Uniform Computer Information Transactions Act or the Uniform Electronic Transaction Act, or for instances of contracts with associates in foreign lands, it is important to address by contract those concerns that are not yet addressed in the law. These contracts may need to cover multi-level, multi-function blends of the pieces that each of multiple parties brings to the table. By forging a good contract on the front end of the transaction, however, the parties can define their own rules that will govern their business dealings.

BASIC CONTRACT CONSIDERATIONS

● Timing of Obligation

–Send Electronic Message

–Receive

–Available in System

–Potential or Actual Review

●An agreement should address the timing of when an obligation arises. An obligation can arise with the receipt or the sending of the electronic message. In some instances mere receipt and availability in the system will suffice, in others receipt and an actual or at least potential review of the message may be appropriate to bind the parties.

BASIC CONTRACT CONSIDERATIONS

●Documents for Binding Acceptance

●Offer Revocation Rights

–Ability

–Timing

●Define Electronic Documents As "Written"

●Bar Use of Lack of Writing As a Defense

●The agreement should define the documents necessary to demonstrate a binding acceptance. The ability and timing of revocation rights with respect to an offer should be set forth as well. Boilerplate language defining electronic documents as "written" and barring the parties from using the lack of a written document as a defense in litigation should be included.

BASIC CONTRACT CONSIDERATIONS

●Define "Signature"

●ID Attribution Procedures

–Validate and

–Attribute Signatures to a Party

●Other contract issues include what exactly the parties will utilize and accept as a "signature" and what attribution procedures will be in effect to validate and attribute those signatures to one or both parties.

BASIC CONTRACT CONSIDERATIONS

●Electronic Records in the Transactions

–Types,

–Storage

–Recording

–Parties' Obligations

●That Agreement Establishes the Course of Dealing Between the Parties

●The types, storage and recording of the electronic records in the transactions should be defined and the parties' obligations with respect to storing and maintaining such electronic communications should be clarified. The agreement should state that it is the agreement that establishes the course of dealing between the parties.

BASIC CONTRACT CONSIDERATIONS

●Website or Domain Name Involved:

–Define Owner of Website Intellectual Property

–Business Entities Try to Vest These Rights

–License Agreement on IP

–Rights to Move the Website to Another Host

●If a website or domain name is involved in the transaction, a good contract will define which party owns the intellectual property associated with the website. A web-site developer may be reluctant to give up its rights to the web-site creation, but wherever possible one of the business entities should at least attempt to vest these rights in itself. If a developer refuses to release such rights, then a license agreement must spell out the business entities' rights to use the intellectual property. Where the website developer and the host are the same, the rights to move the website to another host.

BASIC CONTRACT CONSIDERATIONS

●"Click-Through" or "Click-Wrap" Agreement

●One-Sided and Rarely Read

●But More Unreasonable the Click-Through, the More Likely a Court Will Disregard

–Binding Especially in UCITA Jurisdictions

–Under UCITA, Must Comply With Other Laws Such As Consumer Protection Legislation

●"click-through" or "click-wrap" agreement for the use of the site. The visitor to the website rarely reads the agreement before clicking the "I Accept" icon. As a result, the click-through is generally a bit one-sided in favor of the website. Caution should be exercised, however, because the more unreasonable the click-through, the more likely a court will disregard it as an adhesion contract. The terms and conditions of click-throughs, especially in UCITA jurisdictions, can bind the users or customers and protect the business venture. Such agreements are valid and binding, but under UCITA, they must also be in compliance with other laws such as consumer protection legislation

BASIC CONTRACT CONSIDERATIONS

●Confidentiality Provisions

●Customers' Privacy

●Vendors or Other Parties

●Confidentiality provisions are vital. The various contracting parties are likely to have access to key business information. For example, business partners and website developers would all have access to a company's business strategies and objectives and similar trade information that the business will need to protect. In addition to confidentiality protection, the customers' privacy should also be addressed. Consumers are increasingly attuned to privacy issues and the uses to which their private information are put. Agreements with vendors or other parties to the business venture may entail

confidentiality provisions that your business must meet. All of these should be addressed in the contract.

BASIC CONTRACT CONSIDERATIONS

●Outsourcing Website Development

—Clear Penalties for the Failure to Meet Deadlines

—Protection for Paramount Failures

●With respect to website development, few small and medium sized companies internally develop their own websites. Rather, many entities seem to use specialized website developers rather than their own employees to create the website for the entity. The contract with such a website developer should contemplate several factors and provide clear penalties for the failure to meet any milestone deadlines.

BASIC CONTRACT CONSIDERATIONS

●Outsourcing Website Development

—Warranties on Website Functions

—Refund of Development Costs

—Testing to Insure Website Works

—Firm Deadlines to Go On-line

—Sufficient Penalties for Delays

—Warrant Website Design Does Not Infringe Other's IP

BASIC CONTRACT CONSIDERATIONS

●Branding in e-commerce can be the difference between success and simply being an unknown member of a largely unknown crowd. The domain name is an essential part of branding because the domain name is the link that attaches the entrepreneur to the

customers or buying public. Because domain names are provided on a first come, first served basis, it is imperative that a domain name be identified and secured—both through registration and through trademark protection. While so-called "cyber-squatting," the act of speculatively holding a domain name that is similar to or the actual name of an entity in order to sell that name back to the company at a profit, offers some legal options for attack, the best approach is to identify and secure the domain names as early as feasible.

BASIC CONTRACT CONSIDERATIONS

- Branding Issues

—Domain Name

—Identified and Secured

- Registration and
- Trademark Protection
- BEFORE Substantial Marketing Investment

BASIC CONTRACT CONSIDERATIONS

- Branding in e-commerce can be the difference between success and simply being an unknown member of a largely unknown crowd. The domain name is an essential part of branding because the domain name is the link that attaches the entrepreneur to the customers or buying public. Because domain names are provided on a first come, first served basis, it is imperative that a domain name be identified and secured—both through registration and through trademark protection. While so-called "cyber-squatting," the act of speculatively holding a domain name that is similar to or the actual name of an entity in order to sell that name back to the company at a profit, offers some legal options for attack, the best approach is to identify and secure the domain names as early as feasible.

BASIC CONTRACT CONSIDERATIONS

●Domain Name Ownership

–Multi-Party Arrangement

–Address Change in Players/Website Host

●As far as contract arrangements, pay attention to who owns or controls the domain name. Imagine a multi-party arrangement, for example, where one party provides materials, another operates a "fulfillment center" to market goods that are finished by another party and sold electronically through a website pointed by another party and hosted by still another party. If the contract fails to define the owner of the domain name, then when there is a change in the players of the business venture, or a need to change the host of the website, there may be a dispute as to which party holds the domain name—the source of branding and possibly the only face of the business venture the purchasing public has ever seen.

BASIC CONTRACT CONSIDERATIONS

●Website Host

–Reliability

–Speed

–Performance Standards

–Maintenance Downtime

–Protection From Hacking

–Security Measures

–Data Management and Control

–Redundancy

BASIC CONTRACT CONSIDERATIONS

●Other issues must be considered as far as the host of the website. Reliability and speed are a key difference between a satisfied and a lost customer. Performance standards should be set out and maintenance downtime specified. Protection from hacking and other security measures, data management and control and redundancy that protects the website when there is a failure in a system should all be considered as part of such a contract.

BASIC CONTRACT CONSIDERATIONS

Conclusion

●Upfront Investment Saves Headaches

●Concerns Not Addressed in the Law

●As with any area of the law, a good contract will assist the parties to an electronic venture or transaction by addressing potential concerns and pitfalls and apportioning risk in a manner acceptable to all of the parties. Given that cyberspace law will likely never quite catch up to the technology and innovation that entrepreneurs develop to leverage the technology into the business environment, it is important to address by contract those concerns that are not yet addressed in the law. While these contracts may be complicated, and may combine different functions and responsibilities, a good contract on the front end of the transaction empowers the business players to define their own rules to govern their own business dealings.

DIGITAL SIGNATURES

Uniform Electronic Transaction Act (UETA)

●Uniform National Framework

●Use and Application of Electronic Transactions

● Electronic Fulfill Signed or in Writing

●Each Party Must Agree to Electronic Transaction to Fall Under UETA

DIGITAL SIGNATURES

●The Uniform Electronic Transaction Act (UETA) was adopted by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 29, 1999. The purpose of UETA is to offer a uniform framework of national scope for the use and application of electronic transactions. The Act defines various terms such as "electronic signature," "electronic record," and provides that in general electronic records and signatures satisfy the legal requirement that a record be singed or in writing.Each party to a transaction must agree to the transaction being accomplished through electronic means before UETA will apply.

DIGITAL SIGNATURES

Uniform Electronic Transaction Act (UETA)

●NOT Cover

—Wills

—Codicils

—Testamentary Trusts

—UCC Transactions Optional

—Uniform Computer Information Transactions Act (UCITA) Transactions Optional

DIGITAL SIGNATURES

Uniform Electronic Transaction Act (UETA)

●Format of Electronic Transmission

●Distribution of the Risk of Error

●Retention of "Original" Electronic Records

●Use of "Agents" in Automated Transactions

●Acceptance of E-signatures by Government

DIGITAL SIGNATURES

Uniform Electronic Transaction Act (UETA)

●Electronic Negotiable Instrument

●Called "Transferable Record

●Abolishes the Concept Of:

– Delivery

–Possession

–Endorsement

●Replaced With the "Control"

DIGITAL SIGNATURES

●Under the UETA, a new form of negotiable instrument—an electronic version—is created. This negotiable instrument is labeled as a "transferable record." The UETA abolishes the concepts of delivery, possession, and endorsement. Instead, these ideas are replaced with the concept of "control." Any entity with control over the transferable record qualifies as a UCC §1-201(20) holder during the period of such control and has the same defenses and rights as a holder of a negotiable instrument. Control, for purposes of UETA exists where "a system employed for evidencing the transfer of

interests in the transferable record reliably established that person as the person to whom the transferable record was issued or transferred."

DIGITAL SIGNATURES

Uniform Electronic Transaction Act (UETA)

•Changes Enforceable Contract

•Impacts Article 9 Re: Accounts

•UETA allows contacts that would be unenforceable under standard common law scenarios due to the electronic nature of the documents to be valid and binding. It is also possible that UETA could impact UCC Article 9 issues relating to "accounts." Even under the revised Article 9, which allows a security interest to be perfected by filing, it is not clear the degree of risk that is involved if the instrument is not also possessed.[1] In general, an electronic communication pertaining to an account could fall within the UETA requirements for a "transferable record." This could then allow the person that had control of the communication to fall within the UETA §16(d) provisions offering the rights of a holder under the UCC. Such rights include a priority over the holder of a security interest that is perfected only by filing. The result is that without possession of the transferable record, one could not properly perfect an interest in the account.

FROM "SHRINK-WRAP" TO "CLICK-WRAP AND THE UNIFORM COMPUTER INFORMATION TRANSACTION ACT (UCITA)

"SHRINK-WRAP" and "CLICK-WRAP"

● Shrink wrap—license agreements that can't get to or even see until open the container

● Click-wrap—same license agreements that get on-line at website

DIGITAL SIGNATURES

Uniform Computer Information Transaction Act (UCITA)

●Uniformity in Computer Information Transactions

●Provide for Commercial Practice in Electronic Transactions

–Developed by Agreement

–Developed by Commercial Usage

●The self-stated goal of UCITA is to facilitate and clarify computer information transactions and governing law, including the commercial practice in electronic transactions--to be developed by agreement of the parties and commercial usage.

DIGITAL SIGNATURES

Uniform Computer Information Transaction Act (UTICA)

●Legitimizes the Use of Electronic Agents to Form Binding Electronic Contracts

DIGITAL SIGNATURES

Uniform Computer Information Transaction Act (UTICA)

●UCC Article 2 on Sales Not Cover

—Software Is Transferred to Purchaser

—Purchaser Not Free to Transfer to Others

—Software Transferred w/o Human Intervention

—Software Owner Retains Title As a Licensor

DIGITAL SIGNATURES

●Transactions on the Internet do not neatly fit the sale of goods requirements under UCC Article 2

- The software is transferred to the purchaser, but the purchaser is not free to simply transfer the software to others. In addition, software can be transferred without any human intervention and the owner of the software retains title as a licensor and determines the parameters that control the software's use.

DIGITAL SIGNATURES

Uniform Computer Information Transaction Act (UTICA)

UCITA Addresses:

- Internet-related Mass-marketing Licenses
- Contracts to Download Software
- Access Contracts
- Click-stream
- Click-wrap Agreements

DIGITAL SIGNATURES

- UCITA offices a variety of provisions directed at the technology arena. UCITA addresses internet-related mass-marketing licenses.[1] Under the umbrella of a broadly defined "computer transactions"[2] label, UCITA covers contracts to download software, access contracts,[3] and click-wrap agreements, click-stream, and Web-wrap agreements.[

DIGITAL SIGNATURES

Uniform Computer Information Transaction Act (UTICA)

- Validates the Shrink-Wrap Agreements Accompanying Software and Electronic Data Interchange Transactions

DIGITAL SIGNATURES

South Carolina Secure Electronic Commerce Act

- Electronic Signatures
- Secure Electronic Signatures
- Broad General Application
- The Act addresses issues of electronic signatures and secure electronic signatures and has broad general application.

DIGITAL SIGNATURES

South Carolina Secure Electronic Commerce Act

- Electronic Signatures

"any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the party using it to have the same force and effect as a manual signature."

DIGITAL SIGNATURES

South Carolina Secure Electronic Commerce Act

- Does Not Apply to the Extent "Inconsistent With the Manifest Intent of the Lawmaking Body or Repugnant to the Context of the Same Rule of Law***."
- Does Not Apply to Negotiable Instruments and Other Instruments of Title Where Possession Is Deemed to Confer Title."

DIGITAL SIGNATURES

- The effect of an electronic signature in South Carolina is to satisfy "any rule of law requiring a signature, or providing consequences if a document is not signed."[4] However, the Act does not apply to the extent "inconsistent with the manifest intent of

the lawmaking body or repugnant to the context of the same rule of law***."[5] In addition, the Act does not apply to "any record that serves as a unique and transferable instrument of rights and obligations including negotiable instruments and other instruments of title where possession of the instrument is deemed to confer title."

DIGITAL SIGNATURES

South Carolina Secure Electronic Commerce Act

● A Signature Is "Secure" Where

— Created Pursuant to a Commercially Reasonable Security Procedure Agreed to by the Parties;

—Where Verifiable Under a Government Approved Procedure; Or

DIGITAL SIGNATURES

South Carolina Secure Electronic Commerce Act

A Signature Is "Secure" Where

—The Electronic Signature Is "Unique to the Party Using It" and "Capable of Identifying" the Party, Created Under the "Sole Control" of the Party, and Is "Linked to the Electronic Record to Which It Relates, in a Manner Such That, If the Record Is Changed, the Electronic Signature Is Invalidated"

DIGITAL SIGNATURES

South Carolina Secure Electronic Commerce Act

● Rebuttal Presumptions

—Electronic Record Has Not Been Altered and

—Validity of Any Signature That Is Deemed "Secure"

ENCRYPTION & SECURITY

Network Security

●Firewall

—Hardware Device

—Software

—Filters

ENCRYPTION & SECURITY

●Network security is the system that protects the network from access and interruption by unauthorized users. A "firewall" is the term of art for the basic network security. A firewall "enforces an access control policy between two networks."[1] A firewall is either a hardware device or a program that reviews the information coming through an Internet connection and into a computer system. This information is then filtered and if the incoming information fails to get past the filters, entry to that information is denied The absence of a firewall allows any computer on a networked system attached to the Internet to be directly accessible to anyone on the Internet. A properly equipped person may probe those computers and attempt to access a or utilize those computers.

ENCRYPTION & SECURITY

Network Security

●IPsec

–Cryptographic Security

–"Authentication, Integrity, Access Control, and Confidentiality."

–Works Separately From Applications

●No Program Need Special Configuration

●Encryption "Tunnels"

●In addition, network encryption "tunnels" can be created rendering even computer-to-computer encryption within a network feasible

ENCRYPTION & SECURITY

Network Security

●IPsec

–Beyond Firewall

–Individual Computers Verify Each Other's Identity

–Stops Outside Party Form Observing Intra-computer Traffic

●IPsec addresses issues not covered by a firewall. IPsec allows for the authentication of the "hosts" or computers that are talking to each other to verify the computer with which another computer is communicating. In addition, IPsec allows for encryption to prevent an outside or unauthorized party from observing traffic between computers. Firewalls are not designed to achieve either of these results.[1]

ENCRYPTION & SECURITY

Network Security

●No Protection From What You Allow Into Your Network

●Security Needs to Be Utilized

●At a High Enough Level for Reasonable Protection

ENCRYPTION & SECURITY

●Of course, no security can protect you from what you allow into your network. A firewall that is too loose or executable programs that are received and opened on your system can all pose threats to security.[1] Security is available for a network, but in order

to keep your network secure, that security needs to be utilized and utilized at a high enough level to provide reasonable protection.

●EXAMPLES: system configuration to require many items to come in as attachments—then if open a virus, it is limited and not sent to the entire world

ENCRYPTION & SECURITY

Encryption—How Secret Is Secret?

●Cryptologists' Language

—"Cipher" or "Algorithm"

●Single-Key Algorithms

●Public-Key or Private/Public Algorithms

●"Key"

ENCRYPTION & SECURITY

●As with attorneys, cryptologists have their own language. "Cryptography" is the "art of creating and using methods of disguising messages, using codes, ciphers, and other methods so that only certain people can see the real message."

●A "cipher" or an "algorithm" is a function that will encrypt and decrypt any message, regardless of the text.

●single-key system is one in which both parties use the same key to encrypt and decrypt the message. A public-key system encrypts a message with one key in such a way that only a different key will allow decryption.

●A "key" is a lengthy number "derived from a mathematical algorithm and applied to a randomly-chosen number."[

ENCRYPTION & SECURITY

Encryption—How Secret Is Secret?

●Public-Key System

●Public Key published

●Private Key Confidential

●In a public-key system, the public key is published and known to all. While the private key is held confidential. Messages are sent publicly using the public key, which prevents disclosure of the message contents. Eavesdropping or interception don't matter because the private key needed to decrypt the information is held secretly by the recipient of the information or message.

ENCRYPTION & SECURITY

Encryption— How Secret Is Secret?

●Problems

–Loss of Private Key

●Escrowed With Trusted Third Party

–Secure Key

–Reliable Transmission of Public Key

–ID Lapses in Security

–Stop Use of Public Key After Security Breach

ENCRYPTION & SECURITY

●The private key, however, is also the only means through which the message can be accessed. If the key is lost or destroyed, the information cannot be recovered. Typically, a private key, or the copy of a private key, will be escrowed with another party that is trusted to protect the key and preserve its secrecy.

●Obvious problems are securing the private key from others and remembering or accessing that key. Moreover, there must be a reliable method to publish or transmit the public key to avoid improper encryption and a means must be found to identify lapses in the private key security and to prevent the use of the public key should the private key no longer be secure.

ENCRYPTION & SECURITY

Legislative Efforts

●Cyberspace Electronic Security Act of 1999 (CESA)

–Protects Law Enforcement From Encryption

●Individuals and entities holding encryption keys and providers of the storage of keys provide the encryption key to, or to use that key to decrypt data for, the government when required by a court order or warrant.

●If by warrant, the holder may be prohibited from notifying anyone of the disclosure for 90 days or such other time frame as the court may ultimately extend that prohibition

ENCRYPTION AND ATTORNEY CLIENT PRIVILEGE

CURRENT E-COMMERCE ISSUES

●Privacy of Stored Documents

–*Konop* Case Covered

●Dynamic Pricing

–Segment Market

–Minutiae of Personal Information

CURRENT E-COMMERCE ISSUES

●Price discrimination is the process of charging different customers different prices for identical goods.

●Successful price discrimination requires the segmenting of the market in order to separate different classes of consumers. Today, technology provides minutiae of detail about potential consumers and it is processed instantaneously. In addition, the individual data that is collected about a particular consumer can lead to the online retailers "micro-manag[ing] their marketing and pricing strategies so as to customize nearly every sales offer

●e.g. Amazon charging dif price for same book to "high-end" versus low-end customer

CURRENT E-COMMERCE ISSUES

●Dynamic Pricing

–Anti-Trust Laws

●While federal antitrust laws facially render price discrimination illegal,[1] the reality is that the Department of Justice has not enforced the provision since 1977.[2]

●Moreover, even when enforced the price discrimination provisions were utilized for intermediate suppliers and not to protect the ultimate private consumer.[3] Consequently, it is unlikely that current provisions would be utilized to bar such pricing structures in e-commerce.

CURRENT E-COMMERCE ISSUES

●Article 9 Implications That Change Priorities of Secured Interests

●Defamation and Privacy Issues

CURRENT E-COMMERCE ISSUES

●HIPAA

●HIPAA—addresses confidentiality of medical information

●Issue—stretches to non-med by require med to have same requirements by CONTRACT with anyone they deal with as to confidential information—far more than just not leaving medical records out on the counter

CURRENT E-COMMERCE ISSUES

●Jury Misconduct

—Nov. Case—Fed Dist Ct

—Juror Does Private Internet Research on Corporate Defendant

—Finds Financial Info

—Brings to Deliberations

—1.3 Million Punitives

Document Regarding Internet Domain Names

The Internet can be understood as a network of computers that provides a set of open standards for communicating data and information. To help Web surfers know where they are going, every server that is connected to the Internet has a unique address, known as a domain name. This domain name can either be expressed as a series of numbers or more commonly as a series of letters which we type into the uniform resource locater (URL) box of our Web browsers. To frame the rest of the discussion, one should understand the composition of a domain name. For instance, given www.cnn.com: www stands for World Wide Web, cnn is the second-level domain name, and .com is the top level domain (TLD) name.

There were initially only seven generic TLD's which could be used by companies or anyone else desiring to create a presence on the Internet: .com, .edu, .gov, .int, .mil, .net, and .org. In addition there were over 240 country-code top level domain names (ccTLDs) such as .us for the United States and .uk for the United Kingdom. Given the popularity of the .com TLD and the value in having an easily recognized and memorable domain name, there was initially a flood of applications for .com addresses possessing such qualities. The vast majority of individuals registered sites in which they had a business or personal interest. However, some sought to profit from this process by registering desirable domain names and then sitting on them until legitimate claimants bought them out. This practice became known as cybersquatting.

One of the first cases to deal with this issue arose when Panavision, the well-known photographic camera and equipment business, sought to register panavision.com. Unfortunately, an individual who was a trailblazer in the practice of cybersquatting had

registered the domain name and rather than simply leave the site blank, established a website displaying aerial views of Pana, Illinois. When contacted by Panavision about the company's desire to use the domain name, he demanded $13,000. Rather than pay, Panavision took him to court and won, thus signaling that courts would apply traditional trademark doctrines to the registration and use of domain names on the Internet.

To provide even greater protection to domain names than that afforded by trademark law, Congress passed the Anticybersquatting Consumer Protection Act (ACPA) in 1999. The Act's purpose is to prohibit the bad-faith registration of distinctive marks as Internet domain names by those who intend to profit from the goodwill associated with such marks. In addition, the Act enables courts to cancel or transfer domain name registrations and impose civil penalties against offenders.

Subsequent to the passage of the ACPA, People for the Ethical Treatment of Animals sought to register the domain name peta.org. Much to their shock, when they typed the domain name in their web browser, a website was already in existence entitled People Eating Tasty Animals, complete with links to meat and fur sites. Using the increased legal protections afforded by the ACPA, PETA took the cybersquatter to court and was awarded the domain name.

The agency that administers domain names, the Internet Corporation for Assigned Names and Numbers ("ICANN") requires domain name registrants to be bound by something called the Uniform Domain Name Dispute Resolution Policy ("UDRP"). Pursuant to the UDRP, the domain name holder must submit to a mandatory arbitration proceeding should someone bring a proceeding against it regarding the domain name. It is important to note that either the domain name holder or complainant may submit the

dispute to a court prior to commencement of the arbitration and that the losing party has ten days from the matters conclusion within which they can file a lawsuit.

Another Internet concern many businesses face are generally called "suck sites". This occurs when an individual takes the name of a company or person, adds the word sucks (or various and sundry other word choices), registers the site, and posts a website that has some derogatory material about the entity. A current example involves Chicago Cubs fan Steve Bartman who arguably lost game 6 of the NLCS for his team by interfering with a foul ball. Check out Bartmansucks.com for several parodies involving this unfortunate individual. Individuals such as Mr. Bartman are not alone in this phenomenon; Nikesucks.com, AOLsucks.org and Microsoftsucks.org are all corporate examples of this pervasive trend.

The usual legal protections afforded by trademark law are of little help here since a basic requirement, consumer confusion, is not present. Additionally, barring the presence of defamatory statements, our legal system strongly defends free speech rights. Without legal recourse, what is a company to do? One option is to purchase all derivations of the companies name (companystinks.com, companysucks.com, etc.), thus prohibiting detractors from using the domain names. One prescient example solidifies my view against such a practice.

Verizon followed the aforementioned practice and purchased the domain names Verizon.com and Verizonsucks.com among others. An individual, with an aversion toward Verizon's service and a desire to let the world know, realized that the obvious choices for a suitable website had all been taken. Not willing to give up so easily, he proceeded to make his views known at Verizonreallysucks.com. Upon finding out,

Verizon hired legal counsel to send a cease and desist letter citing the ACPA. The individual then decided to make a point of the absurdity of Verizon's position by purchasing the domain name: VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com. The publicity which followed from such an exchange certainly did nothing to benefit Verizon.

Internet domain names can be a very valuable business commodity. As such, if there is real consumer confusion, companies should vigorously defend their trademark rights via the existing legal mechanisms. However, companies should also be mindful that the Internet is a global soapbox upon which individuals can use their free speech rights to voice their opinions to the masses. As such, it may be wise to divert resources from pursuing legal actions against such site operators and put them toward customer service, thus diminishing the likelihood and scope of such sites.

Document Regarding Intellectual Property Assets

Most businesses believe that the primary value of a company is derived from their tangible assets such as machinery and equipment. However, they often overlook a major component of their market valuation—existing intangible assets, the foremost of which is its intellectual property. The most common mistake small to mid-sized businesses make is thinking they are not large enough to worry about protecting their intellectual property. In the information age, intellectual property can often be the most valuable asset of a company, no matter what its size.

There are three basic steps that an entity should take in order to maximize the value of its intangible assets via the implementation of a systematic intellectual property strategy.

1) The intellectual property (IP) should be identified by conducting an extensive IP audit.
2) The proper method of legal protection should be employed by determining what branch of IP law (trademark, copyright, patent, or trade secret) affords the appropriate protection to the underlying asset.
3) A business-wide internal policy should be established that values and rewards the creation and protection of IP.

The IP Audit

The IP audit must be a comprehensive process that is undertaken across all departments and at all levels of an organization. The various types of IP should be catalogued and eventually evaluated in a formal procedure. Capturing this data will

enable business managers to understand what parts of a company are the primary IP creators so that additional resources can be brought to bear on those divisions. The final component is the establishment of a feasible framework that will identify subsequently produced IP.

Legal Protection

There are four pillars of intellectual property law: trademarks, copyrights, patents, and trade secrets. Based upon the nature of the asset for which protection is sought, one or more of these legal mechanisms can be employed to both protect certain assets of a company and increase the value of a business. Before I discuss the various branches of intellectual property law, be forewarned that these are very simplistic explanations of legal protections that are actually quite complex.

A trademark is a word, name, symbol, or device used to identify the source of a good and distinguish it from the products of another, an example being the Nike swoosh. The creation of a proper trademark allows a company to develop and maintain an identity distinct from that of its competitors, linking the provider of a product to that company's goodwill. Trademarks play a vital role in a company's marketing strategy, moving customers from brand awareness to brand preference and finally to brand insistence. Trademark protection can last indefinitely, as long as certain requirements are met.

Copyright law protects original works of authorship that are fixed in a tangible medium of expression and allows the copyright holder to control the copying of the underlying work. Copyright protection is available only for the manner in which an idea is expressed, i.e. the "work" that is created; the law does not extend protection to the

underlying idea behind the work. For example, if I draft a 2,000 page document that details the process for creating cold fusion, only the diction I use to explain the process (the "work") is protected under copyright law. One can read the document and recreate the cold fusion process (the "idea") based upon my description, and I would be left without legal recourse. A copyright can protect things such as computer databases and computer programs, as long as they possess a minimal level of creativity. Copyright protection exists automatically once the work is fixed in a tangible medium of expression, though significant additional benefits are gained if the copyright is properly registered. Copyright protection lasts for a limited duration, generally the life of the author plus seventy years, though this varies based upon the nature of the underlying work.

Patents are granted for inventions that are new, useful and non-obvious. It is a right granted by the federal government to an inventor, enabling him to exclude others from making, using, selling, or importing the invention within the United States without the inventor's consent. To obtain a patent, one must file an application and have it approved; if granted, the protection generally lasts for a term of twenty years. A patent grants the inventor a market monopoly for a specified duration. After the term expires, anyone can make a replica of the invention and compete in the marketplace. Patents can be obtained for any invention that meets the requirements, including computer programs and novel methods of doing business.

Trade secret law protects information that derives independent economic value from not being generally known to the public, so long as reasonable efforts are employed to maintain its secrecy. Assuming the legal requirements are met, trade secret law can be used to protect data compilations, blueprints, methods of instructions, business plans, and

many other forms of information. One of the most notable examples of a trade secret is the formulation of ingredients that comprise Coca-Cola. One of the most valuable qualities of trade secret law is the fact that it offers protection for a potentially unlimited duration.

Understanding the intricacies of each of these types of legal protections allows for the proper administration of a company's IP strategy.

Internal Policy

This final component of protecting IP assets is the creation of policies and procedures to cultivate the generation of intangible assets within the company. All employees should be informed of the policy, modifications should be made in the personnel manual, and appropriate training should be given. To ensure that the appropriate legal requirements are met, the specific components of the implementation process will depend upon the type of IP that is produced. For instance, it is critical that confidentiality procedures, such as limiting physical access via biometrics or encryption, be implemented to satisfy the requirements for trade secret law protection. For patents, the program should include tangible incentives for employees who create a patentable invention. The end result will be an established structure that enables a business to maintain a culture of creating and protecting valuable IP.

The culmination of a properly administered intellectual property strategy will be the creation of legally transferable and protectable interests, the establishment of a mechanism whereby value can be efficiently gleaned from future creations, and a marked increase in overall market value.

Document Regarding Copyrights, the Internet, and the Open Source Movement

Information is money. Every company recognizes this and works very hard to turn the former into the latter. The traditional method of protecting information has been the legal protections afforded by copyright law. Copyright law generally grants the creator of an original work of authorship which is fixed in a tangible medium of expression the exclusive right to distribute, perform, and display the work for a period of time. Though this period of time varies based upon certain criteria, for most works the present period of protection is the life of the author plus seventy years. After this time period elapses, the work enters the public domain. There are those who argue that this is an inordinate amount of time for information to be kept from the public.

The ability of the Internet to transport information quickly and efficiently has had a tremendous impact on the protection afforded copyrighted works. The pervasiveness of the Internet has fundamentally altered the way information is distributed. The digital nature of the medium allows data to be packaged and sent across telecommunications lines from one point to another at astonishing speed. Because information can be copied and distributed so quickly and easily, the protections afforded by copyrights are increasingly difficult to enforce.

It is primarily the convergence of these two concepts—the extensive period of protection afforded copyrighted works and the ubiquitous nature of the Internet—that has resulted in the advent of the open source movement. The basic concept of open source is that a copyright is not obtained to protect the author's legal interest; rather, the work is given to the public under a less restrictive license. The projects undertaken in the open source model are often quite extensive, lending themselves to the distributive nature of

the Internet. The resources required to complete such a task are distributed to volunteers who freely perform the work on a particular project which is then maintained in a central location.

The modern open source movement began with computer programmers. It was a natural fit for pieces of software code to be written by various decentralized programmers and then compiled in a central location. Today, however; this open source movement has radiated out from its beginnings in the computer software arena and spread to other creations far removed from computer code. It is the belief of those supporting this view that society as a whole should benefit from the work at its inception, not just the original creator.

If you have ever wondered what its like to take a course in Numerical Methods for Partial Differential Equations from the Massachusetts Institute of Technology, now is your chance. The resources available to learn this subject and hundreds of others are available online for anyone. MIT has taken the ideas originating in the open source computer software movement and applied them to the works of authorship created by its faculty—namely, its classes. Developed in 1999, MIT calls this OpenCourseWare (www.ocw.mit.edu).

What makes this project possible is the fact that MIT made an affirmative decision to forgo the rights afforded it under copyright law and instead make the course content available under a license known as the Creative Commons Public License (CCPL). This is one of many license forms which bypass the protections of a copyright and instead opt for a form of protection which allows the public to benefit from information immediately instead of waiting seventy years after the author's demise.

MIT's OpenCourseWare has already had an impact on students in developing countries who would not otherwise be able to attain the knowledge MIT freely distributes as well as students in this country.

While MIT has decided to provide information to the public by foregoing the protections afforded by copyright law on the front end, another organization has approached this task from the opposite end by assimilating works whose copyright has expired. Project Gutenberg (www.gutenberg.net) seeks to "make information, books and other materials available to the general public in forms a vast majority of the computers, programs and people can easily read, use, quote, and search." They accomplish this goal by determining what works have expired copyrights and then having volunteers enter the text of the work into a repository. Shakespeare, Dickens, and thousands of other authors' works are maintained in a database waiting to be freely enjoyed by anyone who downloads them.

There are plenty of other such projects that follow the open source model. For instance, the British Broadcast Corporation (BBC) has stated that it intends to put its entire archive in digital format for the world to freely enjoy (www.bbc.co.uk). Each of these provides tangible examples that clearly demonstrate the power inherent in the open source movement.

The open source movement is in its nascent stages with a tremendous amount of potential, as its principles could be applied to almost any project. The impetus for the open source movement is the length of protection afforded works under copyright law. The capability of performing these projects is provided by the Internet. The end result is the free dissemination of information to the public.

Document Regarding Internet Use Policies

Use of the Internet for activities such as e-mail and web browsing is an integral business tool that increases efficiency. Studies have shown that Americans do the majority of their surfing while at work. This is most obviously due to the high-bandwidth connection most organizations possess allowing for no-wait page loads and nearly instantaneous downloads. Based upon my unscientific observations of my own Internet use and that of my friends, I have come to the conclusion that some percentage of employees' web surfing is not work related.

Certainly your employees are less productive if they are surfing the Net during working hours, right? Not necessarily—it depends upon the nature of the use. They may be using online banking to transfer funds from savings into checking—accomplishing in a matter of minutes what would normally take the entire lunch hour—or linking to a remote camera at their daycare to check on their child as opposed to leaving work or calling to check in. In both cases, the employees are more productive and have higher morale due to the employer allowing personal use of the Internet.

In marked contrast to those benign examples, some Internet use by employees can result in company liability, such as:

- If an employee uses the Internet to access peer-to-peer networks such as Kazaa and transmit copyrighted software without permission of the copyright holder, claims of copyright infringement against the company could result.

- Accessing an insecure site can result in viruses being downloaded into a company network or allow someone on the outside to gain access to a company's computer system.
- If an employee is exposed to sexually explicit material on a computer screen, it can create a hostile work environment.
- Because computer systems identify a user's name and affiliation (i.e. *JohnSmith@WidgetInc.com*), employees leaving messages while logged onto a chat room can result in a statement being attributed to the company. This could lead to claims of defamation, unfair competition or discrimination.
- Because the "cookie" file leaves a trail of all web sites a computer visits, records of inappropriate visits are maintained on the computer and are not actually deleted until it is overwritten by new data. This could be a concern should the computer records be subpoenaed.

These examples are not exhaustive, but they do raise potential liability concerns. That liability is best controlled via two distinct mechanisms: developing a company policy to govern Internet use and the monitoring of employees Internet use.

The first of these is a no-brainer. Every company, no matter how small, should have an established Internet use policy. A well-drafted Internet use policy will have several components. First, create a policy that is grounded in a legitimate business purpose. Set out the reasons behind the policy, the goals of its implementation and the manner in which you seek to accomplish those objectives. The permissible uses of the Internet should be established and the prohibited uses should be enumerated.

Additionally, rules of online behavior and access privileges ought to be discussed. The penalties for failure to comply with the policy should be clearly stated so that there are no misunderstandings. Finally and most importantly, the document must be signed by every employee.

The policy should become part of the personnel manual and given to new employees as part of a standard human resources information package. Periodic reminders should be issued to employees during management meetings and even as pop-ups when users log on.

The second issue, monitoring of Internet use, requires a much more demanding analysis. This issue can be addressed by the use of filtering and monitoring software packages. Of the two, the use of filtering software is an easier decision, as there is almost no downside. Several commercial products are available that simply block certain sites that the company deems inappropriate. Depending upon the level of filtration, there is little likelihood that productivity will decrease as a result or that employees will feel they have an absolute right to visit blocked sites.

Monitoring of Internet use can also be accomplished with the proper software, but though the cost of the software is minimal, the cost of having someone audit user logs can be substantial. Furthermore, a heavy-handed approach would almost certainly result in fairly low employee morale and may make it more difficult to attract future employees. If monitoring is deployed, obtaining written consent from the employee is essential. Incorporating the monitoring guidelines into the Internet use policy and requiring the employee's signature can accomplish this.

One company that has decided against monitoring employees' Internet use is Hewlett-Packard. They also do not use filtering software to block the sites their employees visit, instead relying on the good judgment of their personnel. Such a policy does have its risks, but it has been well received by employees who feel the company respects and trusts them.

The basic issue in crafting an Internet use policy is to find a balance between productivity and liability. Lawyers are fairly adept at finding and addressing potential liability within a company, but only the company knows its workforce well enough to understand what impacts their productivity. By understanding the legal implications and respecting employees' concerns, hopefully the proper equilibrium can be attained.

Document Regarding E-Commerce Basics

E-commerce can be defined quite simply as conducting business on-line. The physical infrastructure that allows e-commerce to occur is based upon two key foundations: the Internet and the World Wide Web (WWW). The Internet can be understood as a network of networked computers that provides a set of open standards for communicating data and information between those computers. The WWW is a set of standard naming and linking conventions that uses the Internet to transport files stored on various computers throughout the network. The combination of the Internet and WWW created an inexpensive infrastructure that replaced private, proprietary networks formerly used by businesses to communicate with each other, thus allowing e-commerce to flourish.

To compete effectively in the new economy, a company needs a viable business model. A company's business model is the manner in which it conducts business in order to generate revenue. As you might imagine, the Internet and WWW have caused companies to create new business models and reinvent old ones. While there are numerous ways in which these new business models could be classified, a common taxonomy includes the following: business-to-consumer (B2C), business-to-business (B2B), consumer-to-business (C2B), and consumer-to-consumer (C2C). B2C e-businesses sell products or services directly to consumers. This is the traditional business model most people think of, an example in the e-commerce world being Amazon.com. B2B businesses sell products or services to other businesses. These companies are usually less well-known to the general public and include businesses such as Chemdex and HoustonStreet.com. C2B business models involve consumers approaching

businesses to purchase goods or services. A popular business following this approach is the reverse-auction site priceline.com. The C2C arrangement involves consumers selling directly to other consumers. The heavyweight in this category is the well-known auction site, E-bay.

Traditionally, business has been conducted in physical buildings, commonly referred to as brick-and-mortar marketplaces. Conventional business models, employed before the Internet became a dominant component of the economic landscape, were limited in two key areas: time and space. Brick-and-mortar institutions are limited in time because the vast majority of them stay open for only a set number of hours per day. Such institutions are also limited in space in that they are located in one physical location, thus limiting the number of potential customers that are likely to shop in such an establishment.

Internet businesses are not constrained by time and space in the same manner. Assuming there is no problem with the underlying technical infrastructure, Internet stores are open 24 hours a day, 7 days a week, 365 days a year. It is just as easy for a customer to place an order at 2 a.m. Eastern Standard time as it is during normal working hours.

The other component, space, is where e-commerce offers pronounced advantages to brick-and-mortar institutions. Any customer with access to a computer that is linked to the Internet can shop at an e-business. The physical location of where the company stocks its goods and the physical location of the customer are basically irrelevant. By going online a business changes its potential customer base from those residing within a fixed proximity from the store's physical location to the entire planet. E-commerce also enables businesses to reach narrow market segments that are too geographically disparate

to capture in a more traditional business approach. This is not to say that traditional brick-and-mortar stores will go the way of the dinosaur, but many will be forced to adapt in some way. An example of this would be so-called brick-and-click stores such as Barnes & Noble that have a strong Internet presence but still maintain their brick-and-mortar locations.

In addition to the increased sales opportunities resulting from a global marketplace and the around-the-clock hours of operation, businesses also have decreased transaction costs due to the low-cost infrastructure provided by the Internet and WWW. Thus, one major impact is to even the playing field, making it easier and less expensive for companies of all sizes to transact business and exchange information.

E-commerce has also caused traditional intermediaries to become obsolete in many cases. Distributors and agents are losing their place in the traditional economy as buyers are linked directly to sellers via the Internet. Their linking function has been replaced in many instances by the underlying infrastructure coupled with user-friendly software.

Another consequence is that buyers now hold more power. Customers have to travel no further than their home PC to compare prices and services from dozens of sellers. This sense of empowerment is also demonstrated as buyers have increased expectations regarding price, comparability, convenience and speed.

One final change brought about by e-commerce, and perhaps the most important, is that the value of information had dramatically increased. Due to the efficient infrastructure provided by the Internet and WWW, processing information has become more powerful and cost-effective than moving physical products. Thus, companies such

as Yahoo! are able to have few employees and physical assets yet still maintain large market share based upon their ability to transfer information in a much more efficient and accurate manner.

By understanding the basic business models that have been created to take advantage of the Internet and WWW, and realizing the alterations in the economic landscape brought about by this new technology, businesses can better position themselves to compete in the e-commerce realm.

Document Regarding Cybersecurity

Conducting business online, commonly referred to as e-commerce, has dramatically altered the way trade is conducted. Two obvious advantages e-commerce businesses have over traditional brick-and-mortar stores are in regards to time and space. The time advantages are clear, assuming there is no problem with the underlying technical infrastructure, Internet stores are open 24 hours a day, 7 days a week, 365 days a year. Regarding space, the physical location of where the company stocks its goods and the physical location of the customer are basically irrelevant. Both of these advantages result from the fact that any customer with access to a computer that is linked to the Internet can shop at an e-business. And it is this constant connectivity of the Internet which results in a major concern to e-commerce businesses—the viruses, worms, and other entities that collectively comprise security risks.

Cybersecurity is not just the stuff of the hyper-concerned, security-conscious business. It is becoming clear that all businesses may have a legal obligation to implement appropriate security measures with regards to their websites. Failure to do so can potentially result in legal liability for the business. In addition to particular designations in statutory laws such as the South Carolina Electronic Commerce Act and the HIPAA Security Regulations, there are several sources which may require that a business maintain certain security measures when transacting business online.

First, a business may be found to have a common law duty to provide reasonable security. Failure to maintain an adequate level of security may result in a breach of that duty and support a cause of action based upon negligence. Just as a business has a duty to use reasonable care when inviting a customer to shop in its store, it can be argued that

a company has a duty to use reasonable security measures when inviting customers to transact business at its website.

Additionally, a business may voluntarily assume obligations to provide a certain level of security. This can be found either expressly or impliedly in contractual obligations due to dealing with third parties. For example, language in the contract may state that Company A will provide "reasonable security" in handling data received from Company B. This voluntary assumption may also be created from representations made in marketing materials or privacy policies of the business. Numerous examples of this can be found in privacy policies on the Internet in which businesses state that they "employ the highest level of security" for all data collected from customers.

Due the increased vulnerabilities faced by businesses engaged in e-commerce and the potential legal consequences, a comprehensive risk management policy is essential to ensure that proper security procedures are implemented and maintained. Such a policy consists of four broad phases: assessment, planning, implementation, and monitoring.

The first phase in a risk management policy is assessment. In this crucial step, a company must determine its objectives so that the broader framework within which the company operates is followed. A complete and accurate inventory should be conducted of all assets. It is important to remember that this includes both tangible (computers, network equipment, etc.) and intangible (trademarks, patents, copyrights, trade secrets) assets on the network. Following this, all reasonably foreseeable internal and external threats should be evaluated; examples include: viruses, worms, denial of service attacks (DoS), buffer overflows, password insecurity, and internal employee theft. Next,

vulnerabilities in the network need to be identified. Finally, the value of each risk enumerated earlier should be quantified so that they can be prioritized.

The second phase of risk management is planning. The primary goal of this phase is to create a security policy, based upon the earlier quantification of risks, that determines which threats are tolerable and which are not. A threat would be tolerable if one of two conditions occurs: either the cost to secure the threat is too high or the risk of it occurring is too low. The first component of this phase is to create a comprehensive information security policy that includes: the safeguards to be introduced, the reason for its implementation, a timeline for its introduction, and the individuals responsible for its installation and maintenance. Next, an audit and review process should be established. This should acknowledge that security is an ongoing activity that needs to incorporate modifications in an organization's objectives, assets, threats, and vulnerabilities so that future changes can be taken into account. Finally, an incident response team and contingency plan should be created to handle any attacks, whether successful or merely attempted, as each of these provide valuable learning opportunities for the organization's security team.

The third phase of risk management is implementation. It is here that particular technologies are selected to counter those threats analyzed in the planning phase. Off-the-shelf software can be purchased or in-house systems can be developed. There are five objectives that the implemented technology should ensure: the confidentiality of the information, the integrity of the information, the authenticity of the information, the availability of the system and information, and that unauthorized access to the information is protected against.

The final phase of e-commerce risk management is monitoring. This is where the success of measures taken is evaluated and modification of unsuccessful measures occurs. Also, the potential of new threats not in existence at the time of the initial assessment is determined, as are any advances in technology that would alter implementation of security measures. An additional consideration is whether there are any new business requirements that would necessitate additional security procedures. A final component of this phase is education of all employees as to proper use of those security measures that have been introduced.

Security is a process as opposed to any particular measure taken. By committing itself to these measures, a company can better position itself from a legal liability perspective and prepare itself for the inevitable security risks inherent in the e-commerce environment.

Document Regarding E-Mail Issues

Few innovations of the information age can rival the usefulness of e-mail. An integral part of the development of the Internet, this was the killer app (popular software application) whose obvious utility heralded the Internet revolution. Businesses soon realized the benefits of this new tool and integrated it into their infrastructure. However, despite the inherent advantages, there can be a downside to this popular form of communication.

The problems that arise from e-mail use in the workplace are a result of certain qualities, both real and perceived, about this medium of communication. These features of e-mail include efficiency, privacy, and permanency.

Efficiency is the prime and very real quality that makes e-mail such a popular method for exchanging information. An individual with the ability to type fairly proficiently can efficiently synthesize his ideas on a particular topic in a matter of minutes and then send them to the intended recipient via the telecommunications infrastructure within seconds.

The second quality of e-mail, one about which most individuals have a misperception, is privacy. Once we draft an e-mail, most of us assume that the only other individuals who will be viewing its contents are those to whom it is addressed. However, unlike a letter sent via the postal service in a sealed envelope, an e-mail involves an intermediate entity—the employer's computer network. Thus, copies of the e-mail exist in several different locations, each of which presents an opportunity for the content to be intercepted.

Furthermore, what's to stop the recipient from sending your e-mail to a third party for whom it was never intended? Consider the plight of Paul Kelly Tripplehorn, Jr. who in June of 2003 sent a rather unflattering e-mail entitled, "you suck," to his former girlfriend who worked with him at a Senator's office. The message was later forwarded to others and due to his choice of content, Mr. Tripplehorn is no longer employed as a Congressional aide. The full text of this dazzling literary work can be found at http://www.angelfire.com/ill/betterthanyou/.

The final misperception most users have about e-mail is its lack of permanence. Once we've read an e-mail and hit the delete button it's gone—right? Wrong. E-mail is an electronic record that exists in various locations on a network system long after the sender and recipient have deleted it. As with other electronic data, it is not truly erased from a system's hard drive until it is overwritten by new data. Pressing the delete button simply clears space on the hard drive that can potentially be overwritten when the computer needs the space. Additionally, copies of the e-mail message reside on not only the sender and recipient's hard drives, but also on any servers through which the e-mail was routed and any back-up tapes that have executed during the relevant time frame. Further dashing the illusion of impermanence, there are numerous software tools that assist individuals in finding e-mails that have been supposedly deleted from a network.

The permanency of e-mail most often rears its head in the context of litigation involving the company. When a business becomes involved in legal proceedings, their attorneys as well as the other party's attorneys can issue subpoenas for all relevant information regarding the lawsuit. In the information age, savvy lawyers are broadening the scope of these subpoenas to include not just tangible items, but also all forms of

electronic data relevant to the lawsuit, including e-mails. Due to its ease of use, the vast majority of individuals treat e-mail content in a much more casual manner than they would an inter-office memo. Given their informal treatment and the permanence of the medium, e-mails can often end up as "smoking guns" that create enormous liability issues for both employees and their companies when discovered by opposing counsel.

Examples abound of instances where e-mails have damaged employees and the companies for whom they work. A fairly recent example involves Henry Blodget, a former Internet company analyst for Merrill Lynch, who sent an e-mail to a colleague in which he referred to Infospace stock as a "piece of junk," despite the fact that he was recommending the stock to his customers at the time. In May of 2003, Merrill Lynch was fined $100 million as a result of this and similar practices, and Mr. Blodget lost his job.

Given these misperceptions and the problems that can arise due to the inappropriate use of e-mail, there are certain steps a company should take to minimize its potential liability. The first is to educate employees on the proper use of e-mail in the workplace. This includes a variety of issues, most of which can be covered by adhering to the following maxim: Treat e-mail as though it were a traditional printed document. Following this proverb will ensure that appropriate content is communicated, eliminate the release of confidential information, and dismiss the misperception of e-mail confidentiality.

Secondly, a company should create a well-designed policy governing e-mail due to the fact that it is a source of potential liability. Components of the policy should include: employee usage guidelines, company discretion in monitoring e-mail use, and

dispute resolution procedures. As with other significant company guidelines, the e-mail policy should be in writing and be acknowledged by employees with their signature.

The final step is to have a well-conceived e-mail retention policy. Most companies (should) have a document retention policy for traditional documents in hard copy. It is essential that a similar policy be in place for information in digital form, such as e-mail. An e-mail retention policy must be designed in advance, with clear justification for the steps to be taken, and provide a reasonable framework for handling outdated digital information.

Understanding the common misperceptions about e-mail can assist a business in both dispelling those improper beliefs and dealing with potential liability issues in a prudent manner.

Figure 1: Screenshot of "Course Overview" View in WebCT

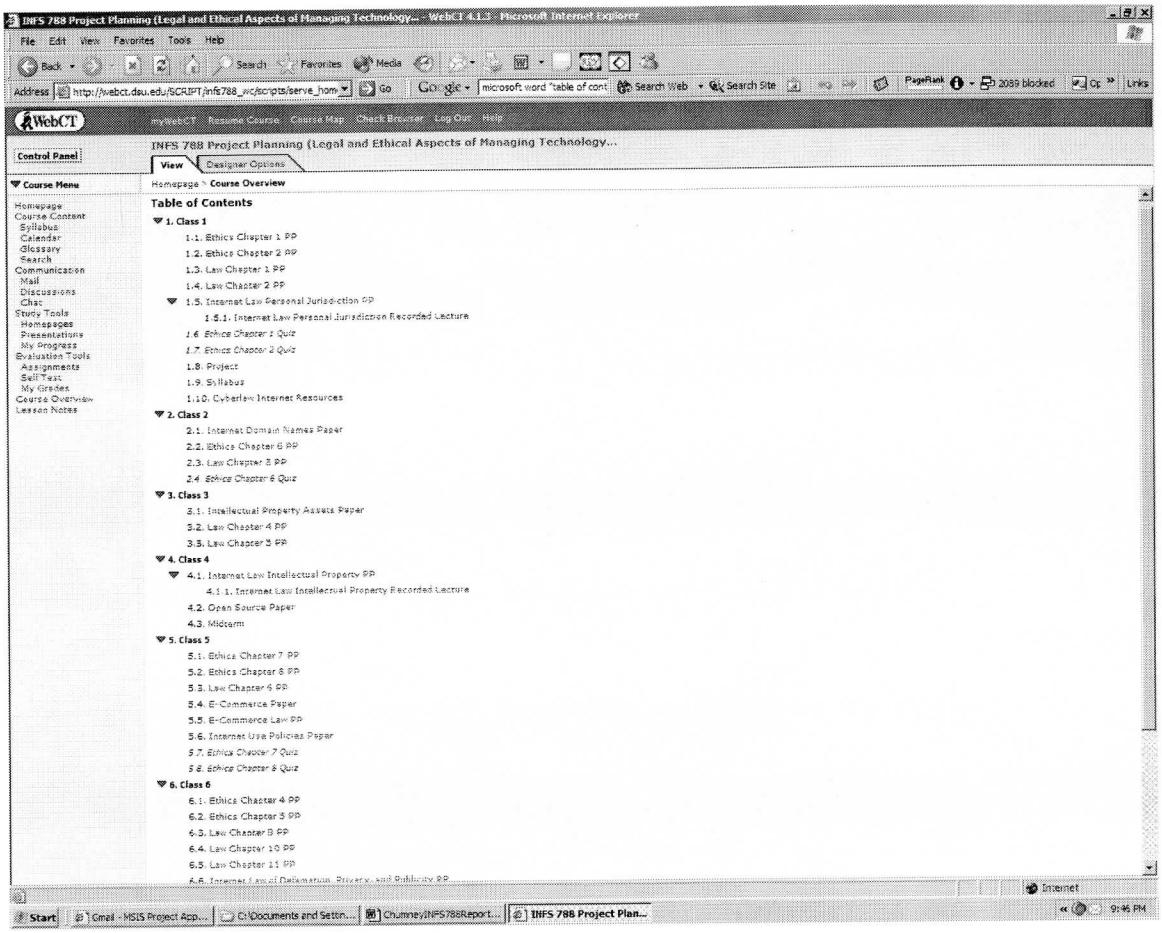


Figure 2: Screenshot of "Homepage" View in WebCT

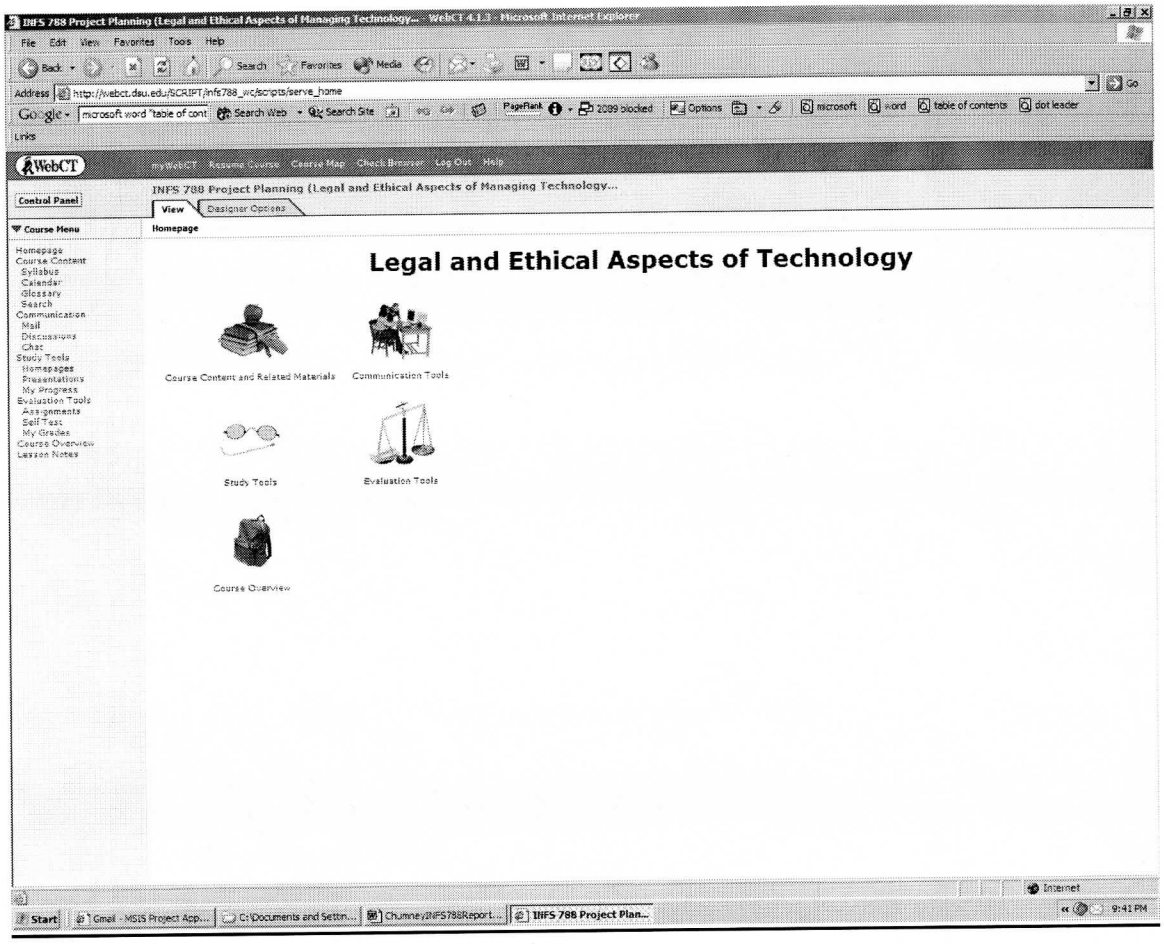


Figure 3: Screenshot of "Course Content and Related Materials" View in WebCT

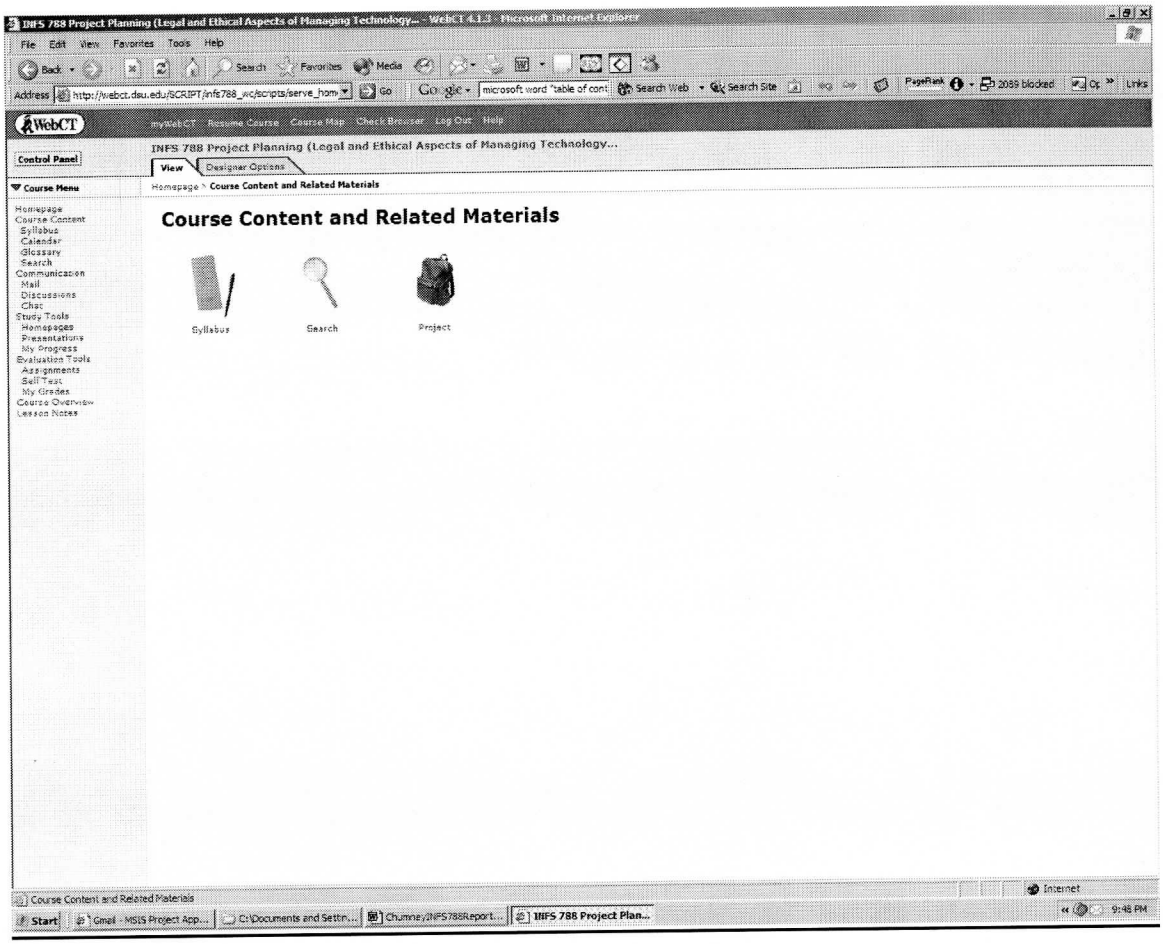


Figure 4: Screenshot of "Communication Tools" View in WebCT

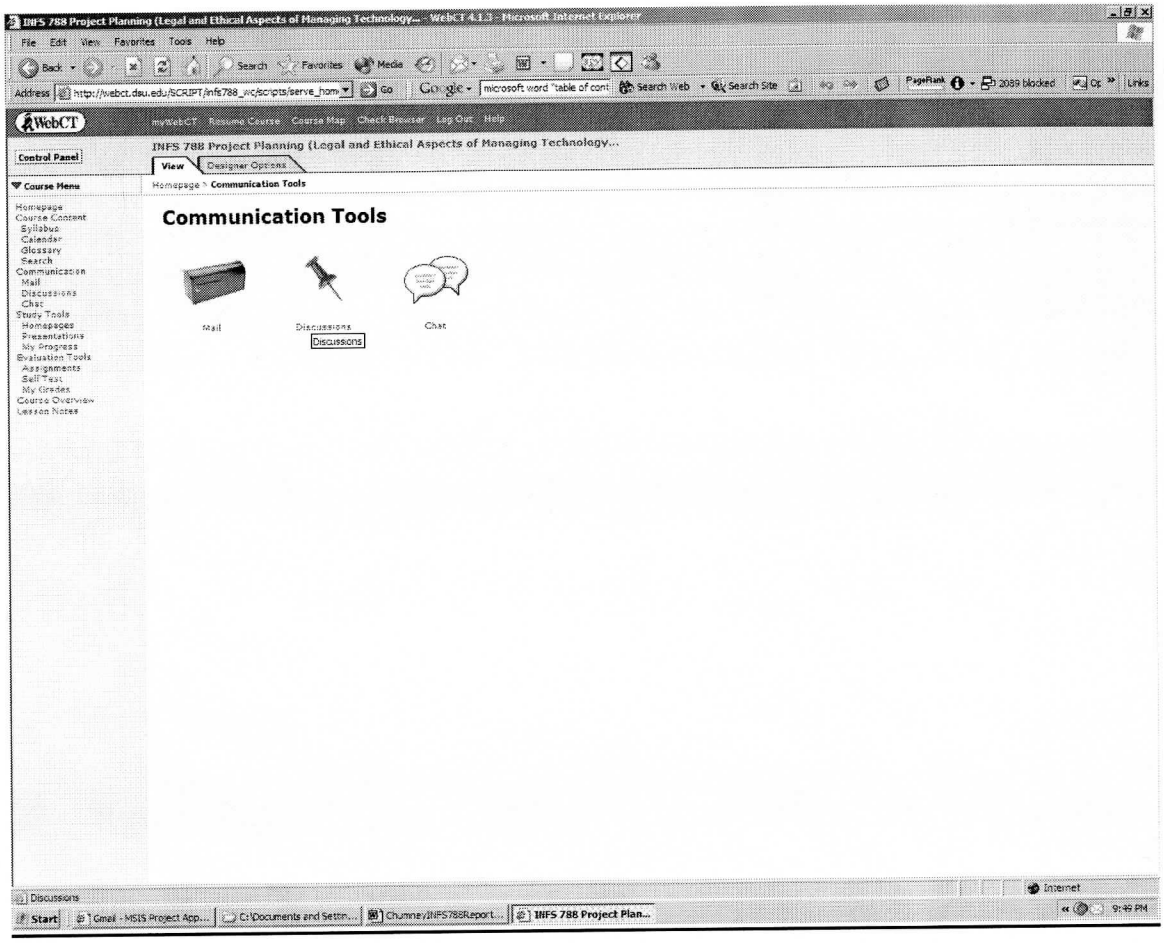


Figure 5: Screenshot of "Discussions" View and "Class 1 Discussion" in WebCT

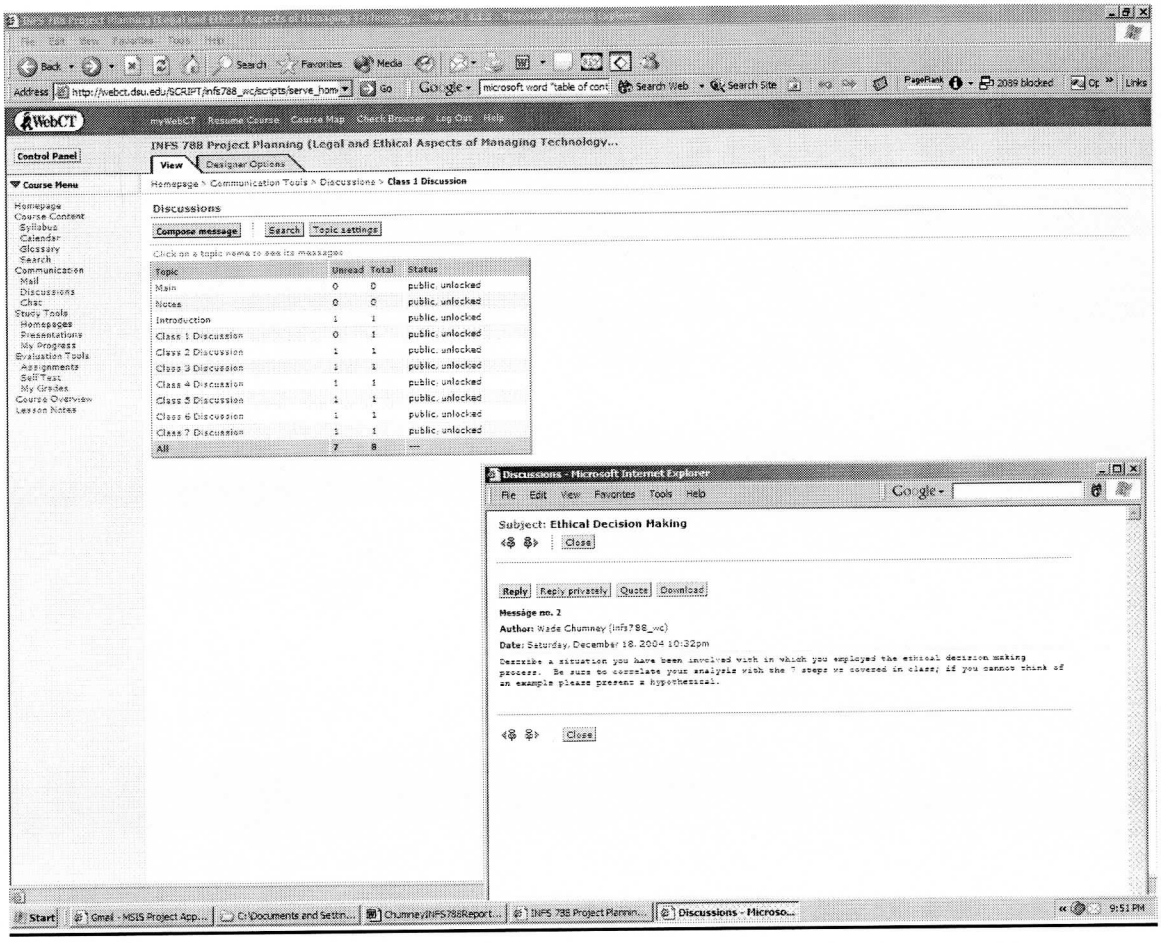


Figure 6: Screenshot of "Study Tools" View in WebCT

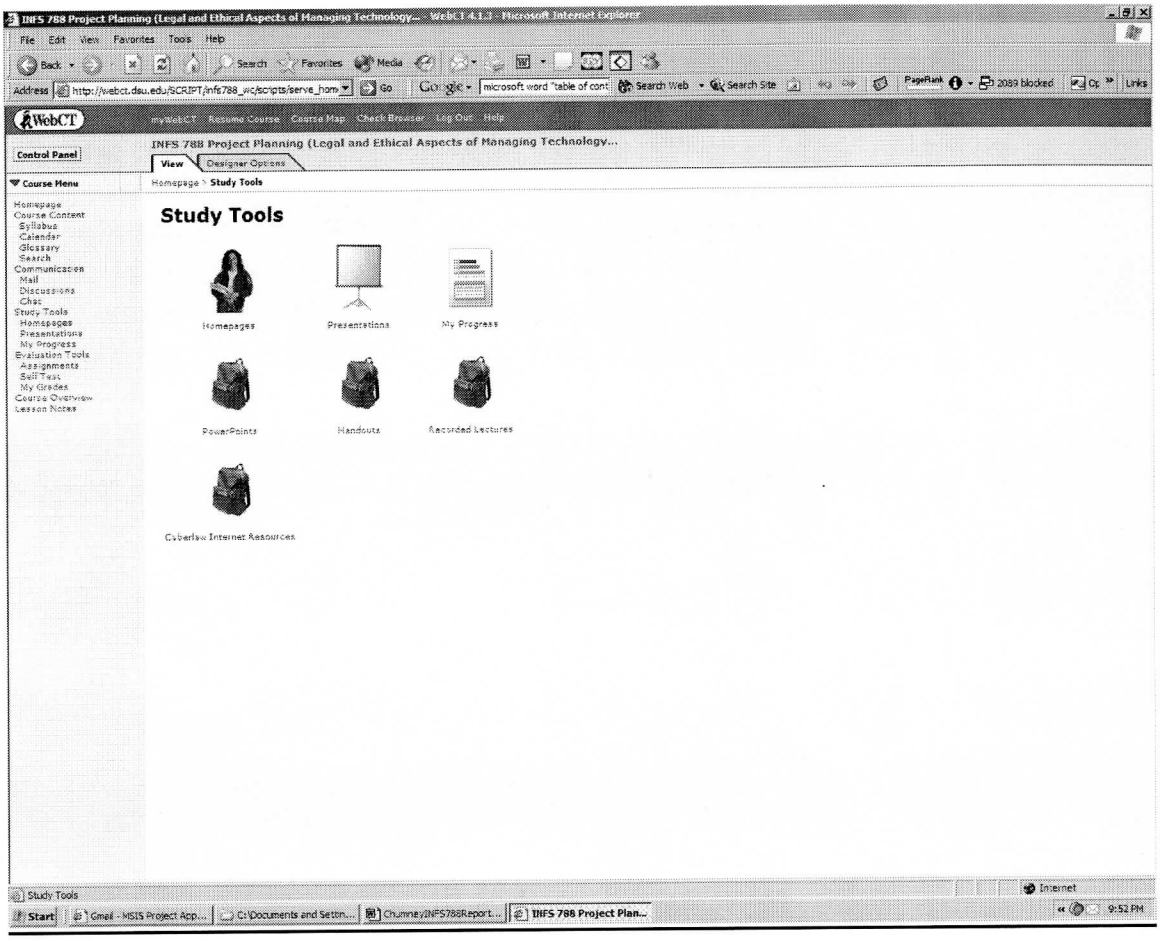


Figure 7: Screenshot of "PowerPoints" View in WebCT

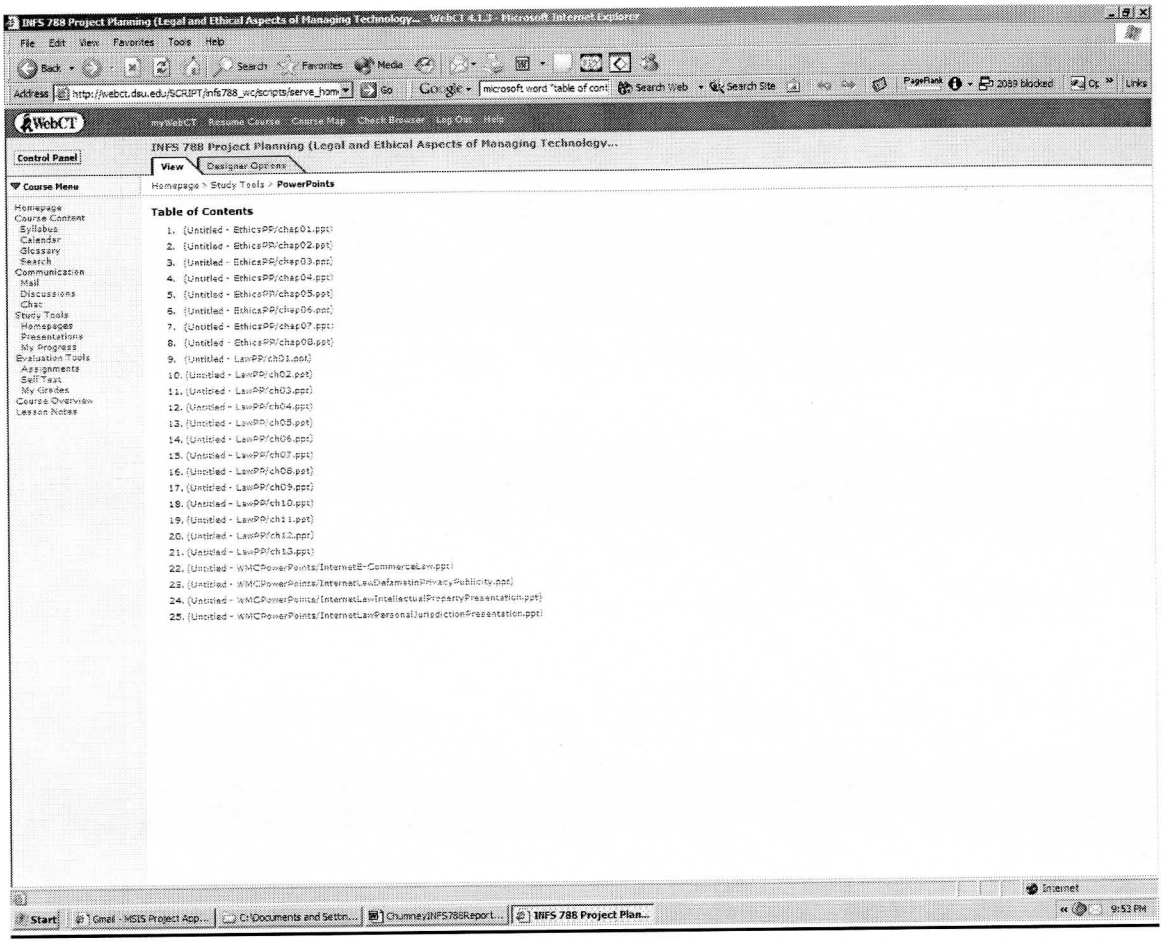


Figure 8: Screenshot of "Evaluation Tools" View in WebCT

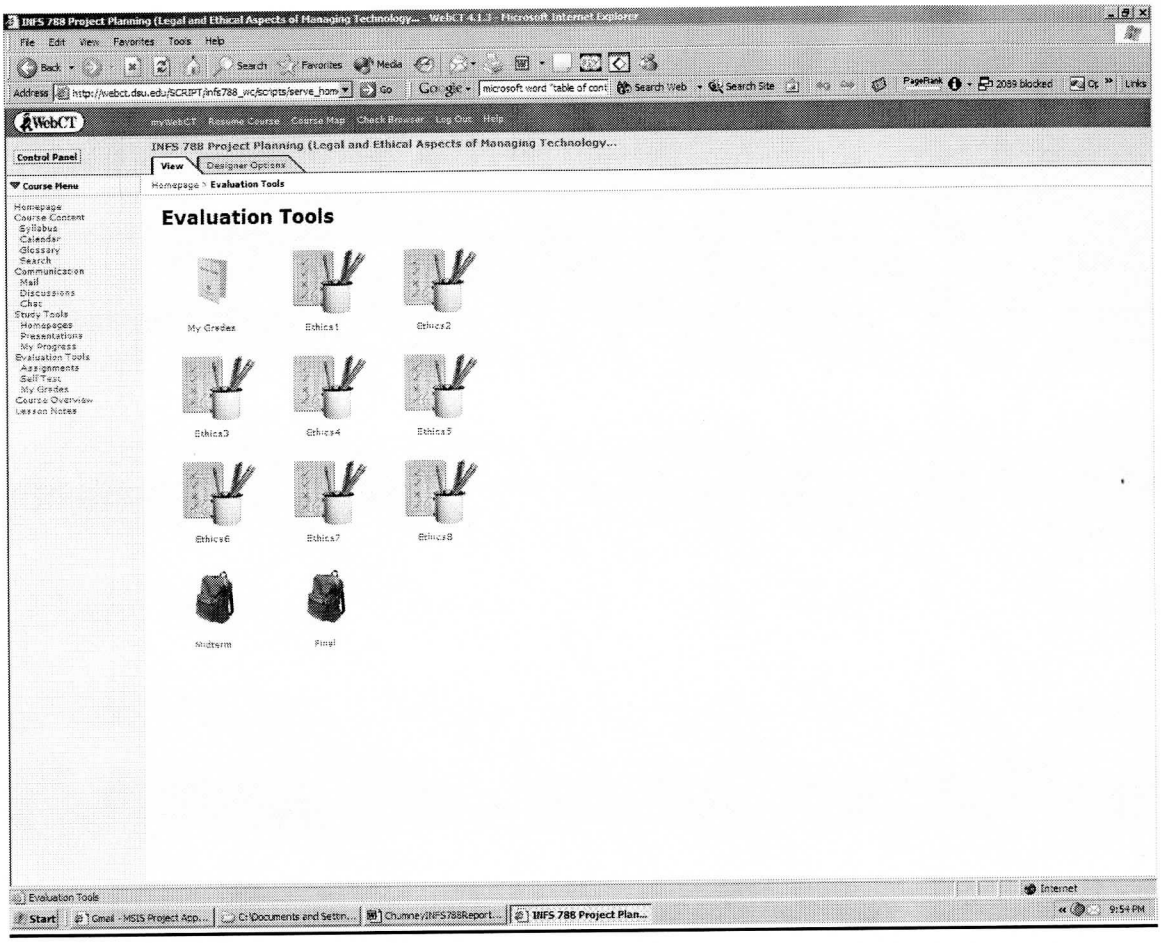
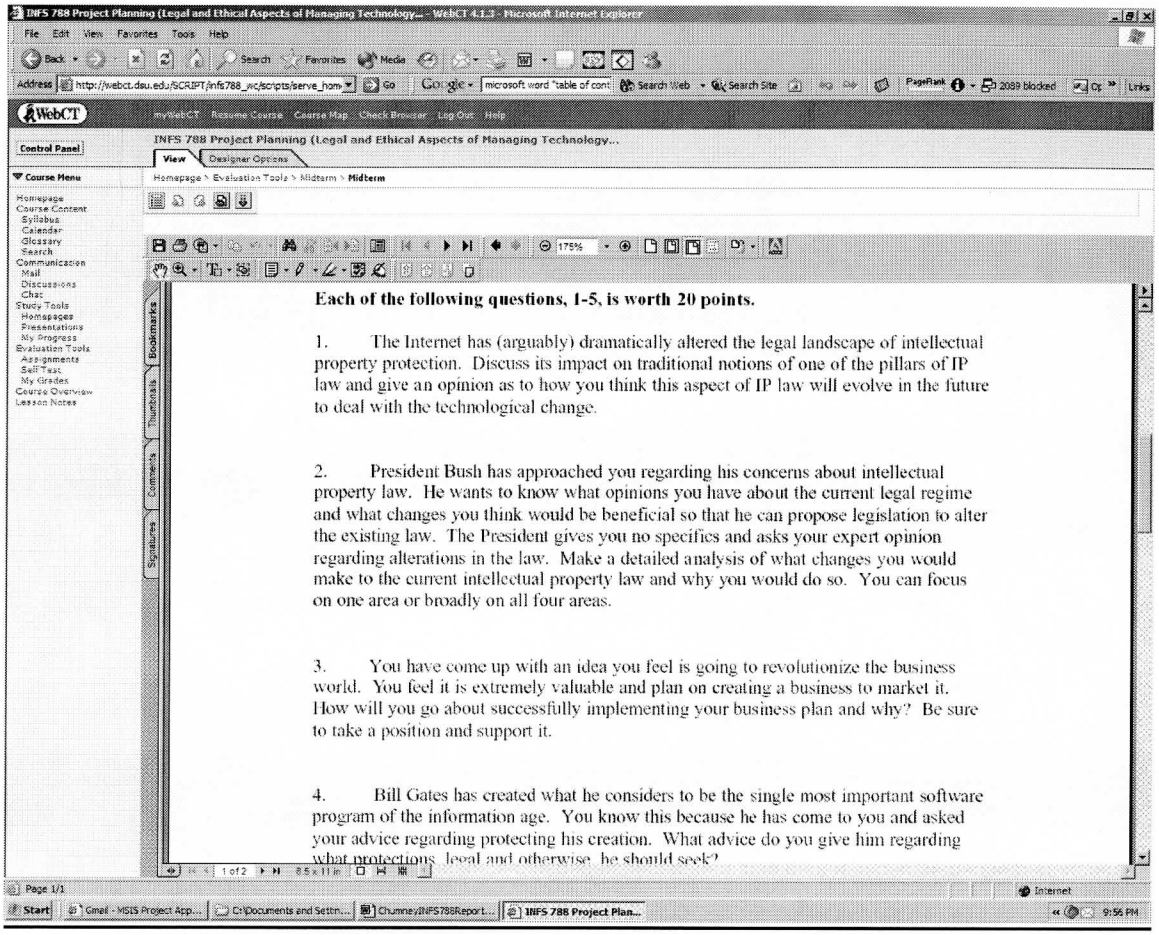


Figure 9: Screenshot of "Midterm" View in WebCT



Conclusion

Ultimately, this project was a complete success. The objective of creating a graduate level distance learning course to be administered via WebCT that meets the criteria established by the Accreditation Board for Engineering and Technology Computing Accreditation Commission (CAC/ABET) was achieved. The anticipated deliverable is now a reality; it is a functioning course on the WebCT server at Dakota State University.

A great deal was learned during the time spent performing the intensive research required to build this course. Today's technology students will be tomorrow's technology professionals. Their ability to comprehend the implications of their work from both an ethical and legal perspective is critical to the success of the technology infrastructure on which this country's economy is built. Without the ability to analyze their decisions properly, technology professionals run the risk of taking actions which are detrimental to both the organizations which employ them and themselves. They open the door to legal liability and worse.

Given the broad scope of issues which had to be researched and synthesized to create this course, there are numerous areas which may require future work. For instance, one issue currently having a tremendous impact on the use of technology is spyware. This is a plague for just about every Internet user today, yet a few years ago it was not even on the radar screen of most people. Currently there are bills before many legislatures attempting to deal with this bane of the Internet and the impact of any potential future laws will not be known for years after their creation. The main reason for this time-lag for the law is that developments in technology are being made at a truly

fantastic pace. The law, and ethics for that matter, always lags behind societal innovations, and the torrid pace at which technology currently moves leaves the established legal framework far behind. The common law of this country has taken centuries to arrive at its present state and statutory law requires consensus from often bitterly divided elected officials. Consequently, the legal framework within which technology develops will always be somewhat antiquated. It is this reactive model of law to technology that ensures there will always remain areas ripe for future research in the law and ethics of technology.

Bibliography

50 Am. Jur. 2d *Libel and Slander* § 275 (1995)

50 Am. Jur. 2d *Libel and Slander* § 276 (1995)

20 S.C. Jur. *Libel and Slander* §55 (1993)

1 U.S.C. § 1127

15 U.S.C. §13(a) (2002)

15 U.S.C. § 1051

15 U.S.C. § 1052(f)

15 U.S.C. § 1065

15 U.S.C. § 1072

15 U.S.C. § 1114

15 U.S.C. § 1121

15 U.S.C. 1125(c)

15 U.S.C. § 1127(a)

17 U.S.C. §102(a)

17 U.S.C. § 102(b)

17 U.S.C. § 103(a)

17 U.S.C. § 106

17 U.S.C. § 107

17 U.S.C. § 117

17 U.S.C. § 201(d)

17 U.S.C. § 201(b)

17 U.S.C. § 302(a)

17 U.S.C. § 502

17 U.S.C. § 504(b)

17 U.S.C. § 504(c)

17 U.S.C. § 505

17 U.S.C. 512(c)(1)(A)

17 U.S.C. 512(c)(1)(B)

17 U.S.C. 512(c)(3)(A)

17 U.S.C. § 1202(a)

17 U.S.C. § 1201(a)(2)

17 U.S.C. § 1201(a)(1)(A)

18 USC §2510 *et seq.* (2000)

18 U.S.C. §2511

18 U.S.C. §2517(4)

18 U.S.C. § 2701(a)

18 U.S.C. § 2711(a)

35 U.S.C. § 101

35 U.S.C. §§ 102-103

35 U.S.C. § 154(a)2

35 U.S.C. § 171

35 U.S.C. § 271

ATPC, slip op., at 3

Fairfax County Circuit Court Record No. 000974, slip op. (Va. Cir. Ct. March 2, 2001)

ICANN International Names (IDN) Committee Briefing Paper On Internet Keyword Issues (February 15, 2002)

Restatement (Second) of Torts, §652A (1977) 192 S.C. 454,7 S.E.2d 169 (1940)

Restatement (Second) of Torts, § 652D cmt. a, at 383 (1977).

Restatement (Third) of Unfair Competition § 25 (1995)

Restatement (Third) of Unfair Competition, §46, cmt. b (1995)

South Carolina Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997)

S.C. Code Ann. §§ 39-8-10 to 39-8-80.

S.C. Code Ann. § 39-8-20.

S.C. Code Ann. § 39-8-50.

S.C. Code Ann. § 39-8-80

South Carolina Code of Laws §26-5-10, *et seq.*, (1976)

South Carolina Code of Laws §26-5-40 (1976)

South Carolina Code of Laws §26-5-30(4) (1976)

South Carolina Code of Laws §26-5-320(A) (1976)

South Carolina Code of Laws §26-5-320(B) (1976)

South Carolina Code of Laws §26-5-510 (1976)

South Carolina Code of Laws §26-5-320(B) (1976)

South Carolina Code of Laws §26-5-530(B) (1976)

South Carolina Code of laws § 36-2-802

S.C. Code §36-2-803.

South Carolina Rule of Professional Conduct 1.6

Uniform Computer Information Transactions Act, Prefatory Note

Uniform Computer Information Transactions Act § 102(a)(1)

Uniform Computer Information Transactions Act § 102(a)(5)

Uniform Computer Information Transactions Act § 102(a)(6)

Uniform Computer Information Transactions Act § 102(a)(12)

Uniform Computer Information Transactions Act § 102(a)(15)

Uniform Computer Information Transactions Act § 103

Uniform Computer Information Transactions Act § 108

Uniform Computer Information Transactions Act § 112

Uniform Computer Information Transactions Act § 112(b)

Uniform Computer Information Transactions Act § 112(e)(2)

Uniform Computer Information Transactions Act § 202

Uniform Computer Information Transactions Act § 206(a)

Uniform Computer Information Transactions Act § 213

Uniform Computer Information Transactions Act § 214(a)

Uniform Computer Information Transactions Act § 214(a)

Uniform Electronic Transaction Act §3(b) (1999)

Uniform Electronic Transaction Act §5 (1999)

Uniform Electronic Transaction Act §7 (1999)

Uniform Electronic Transaction Act §§8-12, 14-16 (1999)

Uniform Electronic Transaction Act §16 (1999)

Uniform Electronic Transaction Act §§17-19 (1999)

Aspen, *The Law of Electronic Commerce* §104[E][4] at 1-32 (1999)

Aspen, *The Law of the Internet"* §8.03(B)(3)

Boss, Amelia H., *Developments on the Fringe: Article 2 Revisions, Computer Contracting and Suretyship*, 46 Bus. Law. 1803 (1991).

Captain, Sean and Cameron Crouch, *Is Your PC Safe From the Enemy Within?* PC World, April 2001.

Crouch, Cameron and Sean Captain, *Is Your PC Safe From the Enemy Within?* PC World, April 2001]

Curin, Matt and Ranum, Marcus J., *Internet Firewalls: Frequently Asked Questions*, §2.1(December 1, 2000) http://www.ranum.com/pubs/fwfaq/

Draft Amendments to the Uniform Computer Information Transactions Act, at new §104 (July 26-August 2, 2002).

Freed, Joel M. and Reynolds, Thomas C. "The New Patent Landscape, Computer and Internet Lawyer 1 at 2 (July 2001).

Friedman, David, *"Does Technology Require New Law?,"* 25 Harv. J.L. & Pub. Pol'y 71 at 71 (Winter 2002).

Froomkin, A. Michael, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, at 713, <http://www.maimi.law.edu/frooomkin/articles/clipper.htm> (visited October 9, 2004).

Graham, Jonathan P., *Note, Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 Tex. L. Rev. 1395, 1405 (1987).

Gurley, J. William "*Cow Decoys Are One Thing: The Trouble with Internet Patents*," Fortune, July 19, 1999, at 118.

Hovenkampf, Herbert, Federal Antitrust Policy: *The Laws of Competition and its Practice* §14.1 (2ed. 1999).

Information Security Committee, American Bar Assoc., ABA Digital Signature Guidelines 35 (1996).

Jenkins, Marylee "*The Latest Word on Trademarks and Domain Names*," The 17th Annual Intellectual Property Law Conference at 1088-89 (April 11, 1085).

Keeton, W. Page *et al., Prosser and Keeton on the Law of Torts*, §111, at 771 (5th ed. 1984).

Kindel, Christopher M., "*Survey of Developments in North Carolina Law and the Fourth Circuit*," 1999, 78 N.C. L. Rev. 2105 at 2141.

Khan, Seema A., "*Emerging Technologies: A Legal Tool Kit for Responding to Resulting Intellectual Property Issues*", 2002.

Lando, Peter R., "*Business Method Patents: Update Post State Street*," 9 Tex. Intell. Prop. L. J. 403 at 418.

McLaughlin and Cohen, *Commercial Law: Electronic Transactions,* The National Law Journal, December 13, 1999, at B6.

McKeon, , Robert W., Jr., Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena, 12 J. Marshall J. Computer & Info. L. 511, 512-514 (1994).

Madison, Michael J., "*Click-Through Agreements and the Emerging Law of Access*," The 17th Annual Intellectual Property Law Conference Course Materials at 1135-36 (April 11, 2002.

Nimmer, Raymond and Ring, Carlyle C., *Issues Memorandum for Proposed Amendments to UCITA*, July 12, 2002, at p. 1.

Pain, Steve, "*E-Business: Price of being Framed on the Internet*," Birmingham Post, Feb 27, 2001 p. 24.

Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960)

Ramsay, John T., E*lectronic Commerce: Cryptography and the Law*, at 7

Ranum, Marcus J. and Curin, Matt, *Internet Firewalls: Frequently Asked Questions*, §2.1 (December 1, 2000) http://www.ranum.com/pubs/fwfaq/

Reynolds, Thomas C. and Freed, Joel M., "The New Patent Landscape, Computer and Internet Lawyer" 1 at 2 (July 2001).

Ring, Carlyle C. and Nimmer, Raymond *Issues Memorandum for Proposed Amendments to UCITA*, July 12, 2002, at p. 1.

Ritter, Jeffrey B., *Software Transactions and Uniformity: Accommodating Codes Under the Code*, 46 Bus. Law. 1825 (1991).

Rustad, Michael L., Symposium: Uniform *Computer Information Transaction Act: Article Making UCITA More Consumer-Friendly*, 18 J. Marshall J. Computer & Info. L. 547, 564 (1999).

Sanchez, Veronica M., Comment, *Taking a Byte Out of Minimum Contacts: A Reasonable Exercise of Personal Jurisdictionin Cyberspace Trademark Disputes*, 46 UCLA L. Rev. 1671 at 1671-72 (1999).

Slonim, Burt L., *E-Mail and Privileged Communications,* N.Y. L.J., November 17, 1997, at S3 and S13.

Smart, Patrica S, "*Infringement in Cyberspace*," The 17th Annual Intellectual Property

Law Conference Course Materials at 1069, 1073, 1075, 1076, 1082 (April 11, 2004)

Tyson, Jeff, *How Firewalls* Work, at 2, (last visited October 7, 2004),

http://www.howstuffworks.com/firewall1.htm

Using IPsec (IP Security Protocol) §13.2 http://www.openbsd.org/faq/faq13.html#What (Last Visited October 11, 2004).

Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890)

Warren & Brandeis, 4 Harv. L. Rev. at 195

Warren & Brandeis, 4 Harv. L. Rev. at 210-11.

Weis and Mehrotra, *On-line Dynamic Pricing: Efficiency, Equity, and the Future of E-commerce*, 6 Va. J.L. & Tech. 11, 12 (2001).

ALS Scan v. Remarq Communications, Inc., 239 F.3d 619 (4th Cir. 2001)

ALS Scan, Inc. v. Digital Service Consultants, Inc., et al., 293 F.3d 707 (4th Cir. 2002)

Abofreka v.Alston Tobacco Co., 288 S.C. 122, 341 S.E.2d 622 (1986)

Accord, Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985).

Amazon.com, Inc. v. Barnesandnoble.com, Inc., 73 F. Supp. 2d 1228 (W.D. Wash 1999).

Amazon.com, Inc. v. Barnesandnoble.com, Inc., 239 F.3d 1343 (Fed. Cir. 2001).

Asahi Metal Ind. Co., Ltd. v. Superior Court, 480 US 102 at 112, 107 S.Ct. 1026 at 1032.

Aviation Associates and Consultants, Inc. v. Jet Time, Inc., 303 S.C. 502, 402 S.E.2d 177 (1991).

Bell v. Bank of Abbeville, 208 S.C. 490, 493-94, 38 S.E.2d 641, 643 (1946).

Bernia of America, Inc. v. Fashion Fabrics International, Inc., 57 USPQ 2d (N.D. Ill. 2001).

Bihari v. Gross, 119 F. Supp. 2d 309 (S.D.N.Y. 2000).

Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 at 1045 (9th Cir.1999).

Brown v. Geha-Werke GmbH, 69 F. Supp. 2d 770 (D.S.C. 1999), citing Elliott Mach. Corp. v. John Holland Party, Ltd., 995 F.2d 474 (4th Cir. 1993).

CEG Stoval v. O'Connell Associates, Inc. 84 F.3d 132, 135 to 136 (4th Cir. 1996), cert. denied 117 S. Ct. 437 (1996).

Coach Leatherware Co., Inc. v. Ann Taylor, Inc., 933 F.2d 162 at 168 (2d Cir. 1991).

Columbia Briar Gate Co. v First National Bank of Dallas, 713 F.2d 1052, 1057 (4th Cir. 1983).

Computer Care v. Service Systems Enterprises, Inc., 982 F.2d 1063 (7th Cir. 1992).

Constant v. Spartanburg Steel Prods., Inc., 316 S.C. 86, 447 S.E.2d 194 (1994) 181 S.E.2d 325 (1971).

Conwell v. Spur Oil Co., 240 S.C. 170, 125 S.E.2d 270 (1962).

Doe v. Rostker, 89 F.R.D 158, 161 (N.D. Cal. 1981).

ESAB Group, Inc. v. Centricut, L.L.C., 34 F. Supp. 2d 323 (D.S.C. 1999).

ESAB Group, Inc. v. Centricut, Inc., 126 F.3d 617, 623-24 (4th Cir. 1997), cert. denied, 523 U.S. 1048, 118 S.Ct. 1364 (1998).

Elder v. Gaffney Ledger, 341 S.C. 108, 113-14, 533 S.E.2d 899, 901-02 (2000).

Eubanks v. Smith, 292 S.C. 57, 354 S.E.2d 898 (1987).

Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 361 (1991).

Fleming v. Rose, 338 S.C. 524, 526 S.E.2d 524 (Ct.App. 2000).

Ford Motor Co. v. 2600 Enterprises, 01-CV-71685-DT (E.D. Mich. Dec. 20, 2001).

Fulton v. Atlantic Coast Line R.R., 220 S.C. 287, 67 S.E.2d 425 (1951*) cf. Woodward*, 277 S.C. at 32-33, 282 S.E.2d at 601.

Gertz v. Robert Welch, Inc., 418 U.S. 323, 325, 94 S.Ct. 2997, 3000, 41 L.Ed.2d 789, 797 (1974).

Ticketmaster Corp. v. Microsoft Corp., Case No. 97-3055 (C.D. Cal. Complaint filed Apr. 28, 1997).

Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763 (1992).

Tyler v. Macks Stores, 275 S.C. 456, 272 S.E.2d 633 (1980).

U.S. v. M/V Santa Clara I, 859 F. Supp. 980 at 987 (D.S.C. 1994).

"*Uniform Domain Name Dispute Resolution Policy*," found at http://www.icann.org/dndr/udrp/policy.htm.

Universal City Studios, Inc. v. Corley, 273 F.3d 429, 60 (2d Cir. 2001).

Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

Vinten v. Jeantot Marine Alliances, S.A., et al., 191 F. Supp. 2d, 642 (D.S.C. 2002).

Vivendi Universal v. Sallen, WIPO D2001-1121 (Nov. 7, 2001).

Wardlaw v. Peck, 282 S.C. 199, 318 S.E.2d 270 (Ct.App. 1984).

Washington Post Co. v. Total News, Inc., 97 Civ. 1190 (PKL) (S.D.N.Y. complaint filed Feb. 20, 1997).

Wells American Corp. v Sunshine Electronics, 717 F.Supp. 1121, at 1125 (D. S.C. 1989).

Woodward v. South Carolina Farm Bureau Ins. Co., 277 S.C. 29, 282 S.E.2d 599 (1981).

Wright v. Sparrow, 298 S.C. 469, 381 S.E.2d 503 (Ct.App. 1989).

Zacchini v. Scripps-Howard Broadcasting Company, 433 U.S. 562, 97 S.Ct. 2849, 53 L.Ed. 2d 965 (1977).

Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 at 1124 (W.D. Pa, 1997).