Volume 3, Numbers 1 and 2 **ISSN 1554-5393**

JOURNAL OF STRATEGIC E-COMMERCE

An official Journal of the
Allied Academies, Inc.

David Wyld
Co-Editor
Southeastern Louisiana University

Randall Settoon
Co-Editor
Southeastern Louisiana University

Academy Information
is published on the Allied Academies web page
www.alliedacademies.org

The Allied Academies, Inc. is a non-profit corporation chartered under the laws of North Carolina in the United States. The Academy is an association of scholars and practitioners whose purpose is to advance the knowledge, understanding, and teaching of e-commerce and e-government throughout the world.

Whitney Press, Inc.

Printed by Whitney Press, Inc.
PO Box 1064, Cullowhee, NC 28723
www.whitneypress.com

Authors provide the Academy with a publication permission agreement. The Allied Academies is not responsible for the content of the individual manuscripts. Any omissions or errors are the sole responsibility of the individual authors. The Editorial Board is responsible for the selection of manuscripts for publication from among those submitted for consideration. The Editors accept final manuscripts in digital form and the Publishers make adjustments solely for the purposes of pagination and organization.

The *Journal of Strategic E-Commerce* is published by the Allied Academies, Inc., PO Box 2689, 145 Travis Road, Cullowhee, NC 28723, USA, (828) 293-9151, FAX (828) 293-9407. Those interested in subscribing to the *Journal*, advertising in the *Journal*, or otherwise communicating with the *Journal*, should contact the Executive Director at info@alliedacademies.org.

JOURNAL OF STRATEGIC E-COMMERCE

Volume 3, Numbers 1 and 2

JOURNAL OF STRATEGIC E-COMMERCE

Volume 3, Numbers 1 and 2

JOURNAL OF STRATEGIC E-COMMERCE

CONTENTS OF VOLUME 3, NUMBER 1

JOURNAL OF STRATEGIC E-COMMERCE

CONTENTS OF VOLUME 3, NUMBER 2

LETTER FROM THE EDITORS

Welcome to the *Journal of Strategic E-Commerce.* We are extremely pleased to be able to present what we intend to become a primary vehicle for communication of e-commerce issues throughout the world.

The Allied Academies is a non-profit association of scholars and practitioners in entrepreneurship whose purpose is to encourage and support the advancement of knowledge, understanding and teaching of e-commerce throughout the world. The *Journal of Strategic E-Commerce* is a principal vehicle for achieving the objectives of the organization. The editorial mission of this journal is to publish empirical and theoretical manuscripts which advance the e-commerce initiatives. To learn more about the Academy, its affiliates, and upcoming conferences, please check our website: www.alliedacademies.org. We look forward to having you share your work with us.

David Wyld
Randall Settoon
Southeastern Louisiana University

ARTICLES for Volume 3, Number 1

ARTICLES for Volume 3, Number 1

ELECTRONIC MUSIC DOWNLOADS: WHAT'S AN INDUSTRY TO DO?

R. Nicholas Gerlich, West Texas A&M University
Nancy Turner, West Texas A&M University
Pamela H. Wilson, Consultant, Amarillo,Texas

ABSTRACT

Electronic music downloads (EMDs) continue to generate controversy in the recorded music industry. In the first years of the 21st century, sales of pre-recorded CDs plummeted, and were blamed in part on peer-to-peer (P2P) file-sharing of songs by individuals. The Recording Industry Association of America (RIAA) has filed suit against thousands of persons engaged in allegedly illegal file-sharing. In the past two years, numerous pay-per-song sites have emerged, offering people a legal way to acquire recorded music. Portable digital music devices such as iPod interface easily with computers as well as legal download sites, making digital music a powerful force in the market. In Spring 2005, news reports indicated that industry executives were considering increasing the price of music downloads. Furthermore, in spite of selling 300 millions songs legally in 2004, the number of pirated songs stayed the same as in previous years. Thus, legal music download sites do not appear to be slowing the volume of illegal song sharing. In this study we surveyed college students to assess their past and current music downloading practices, their intentions to utilize pay services for music, and their perceptions of lawsuits filed by the industry. We conclude by offering recommendations for the industry.

INTRODUCTION

Electronic music downloads (EMDs) have generated controversy in the recorded music industry. A reduction in sales of prerecorded CDs has been blamed in part on peer-to-peer (P2P) file-sharing of songs by individuals.[1] During Senate Hearings on the subject in September 2003, the head of the Recording Industry Association of America (RIAA) cited statistics showing a drop of 26% in recorded music shipments from 1999 to 2002 and sales of top ten selling albums down from

60 million units in 2000 to 34 million in 2002.[2] The RIAA has filed suit against thousands of persons engaged in allegedly illegal file-sharing and has faced vast amounts of criticism for their approach to enforcement of copyright laws. Numerous pay-per-song sites have emerged, offering people a legal way to acquire recorded music.

In this study we surveyed college students to assess their past and current music downloading practices, as well as their intentions to utilize pay services for music. We review the legal causes of action the music industry has taken against individual users, analyzing the reality of a recovery against individual down loaders, and compare this with current student perceptions. We also address whether the industry's legal efforts have been effective in discouraging file-sharing.

The internet makes the world accessible at our fingertips. Where once we were limited to listening to music played on the local radio station or purchased in the form of a "record", we can now have nearly any work by any artist on our desktop at a moment's notice. Unfortunately, the programs first developed for providing this music were not in alliance with the copyright laws written to protect the property rights of the writers and owners of the works and to allow compensation for their artistic expression. Senator Susan M. Collins notes in her statement before the Senate Hearings on the matter of file-sharing, that the notion that "if you can find it on the internet, you can have it", is prevalent across our society.[3] This is really part of the wider notion, necessarily addressed in all college ethics courses today that "if it can be done, it should be done." It imperative that we educate university students on the implications of the law, as well as their ethical responsibilities, though these may contradict this notion that they have become so comfortable with. On the one hand, it may be determined unethical for the RIAA to go about suing their own customers as a means of getting a message across.[4] Some may even blame the alleged infringement on the industry for providing the necessary tools and for not enforcing the law earlier.[5] On the other hand, the industry does have the legal right to enforce the laws that were, in fact, written for the purpose of protecting the owner of the material.

WHY ARE THEY PICKING ON US?

In the now infamous Napster lawsuit that dominated headlines in 2001 and 2002, several record companies obtained an injunction and a shut down order against Napster, based on allegations of continual infringement of copyrights the companies held.[6] The liability of Napster was based on two theories of copyright

liability – contributory infringement and vicarious infringement.[7] The Federal 9th Circuit Court of Appeals, based in California, had held in an earlier appeal that Napster would be guilty of contributory infringement where they learned that specific infringing material was available on their system and did not purge the material.[8] In addition, the company was vicariously liable because they had the right and ability to supervise the infringing activity, and a financial interest, yet did nothing to stop it – somewhat like an employer's responsibility for its employee's actions.[9] Napster had "failed to exercise [its right to police its system and] prevent the exchange of copyrighted material."[10] In the 2003 case against Aimster, the 7th Federal Circuit Court of Appeals followed suit, finding that while internet service providers (ISPs) cannot practicably be held accountable for every instance where a copyrighted piece of information travels over their service, as recognized by the "safe harbor" provision of the Digital Millennium Copyright Act (DMCA), Aimster actually encouraged, rather than discouraged, infringement.[11] The Court made clear that the safe harbor provisions for ISPs were not intended to completely eliminate contributory liability for copyright infringement.[12]

At the end of round one, then, the record industry had a strong lead. As technology goes, however, things changed very quickly. Specifically, companies developed software utilizing a decentralized index model for peer to peer file sharing, rather than the centralized model Napster had used. The Napster software utilized a collective index of files available for copying which was maintained on its servers.[13] In order to obtain a digital copy of a recording, the user would send a search request to the Napster server that would then conduct the search and send the results.[14] In addition, Napster provided technical support, a chat room and a directory for artists.[15] The Grokster program does not entail so much activity by the provider. In using Grokster's "supernode" or "FastTrack" technology, originally developed by KaZaa, a person seeking to download a work is connected to the most accessible "supernode", an individual computer on the network designated as an indexing server.[16] Grokster is not in the picture at that point; it has merely provided the software capability. Gnutella, on the other hand, is an "open-source" software, where the search literally goes out directly to all computers on the network.[17]

The music industry pursued action against the providers of these decentralized software programs in the now highly controversial "Grokster" case.[18] However, contrary to their prior success, the record industry hit a brick wall this time in the courts. The trial court held, and the 9th Circuit Court of Appeals agreed in its August 2004 decision, that the program providers were not liable for contributory infringement because the programs, though certainly potentially

utilized for illegal purposes, had "significant noninfringing uses."[19] The Grokster court relies heavily on the Betamax case, regarding liability of VCR producers, in its finding against contributory liability.[20] The 9th Circuit further recognizes that it has rejected the test used by the 7th Court of Appeals in Aimster, which based its decision on how probable the infringing use of the program was.[21] Finally, the Grokster court found that the program developers were not vicariously liable for the copyright infringement by users because, as opposed to earlier cases, the program developers here did not retain control or supervision over the use of the program.[22] In quoting the Supreme Court's Betamax decision, the 9th Circuit calls on Congress to make necessary changes to the intellectual property laws, noting that it is not for the courts to make such laws.[23] Round two goes to the P2P advocates, or, at least, the software developers.

The door is not completely closed on liability for servers or software distributors. The courts recognize that the "safe harbor" provisions of the DMCA are not iron clad. In addition, as noted above, there remains a contradiction in the courts of appeal regarding the standard for contributory liability. The Grokster decision is being appealed to the U.S. Supreme Court by the recording industry, which claims the 9th Circuit is allowing Grokster and Steamcast to "brazenly profit from infringement", with a very large amount of interest from outside groups in addition to the thousands of plaintiffs already involved.[24] Given the conflict between the circuit courts and the high level of interest in the case, it would seem that we should see a decision from the high court on the issue, though it may be some time before the case is considered. In the meantime, the music industry has apparently decided to pursue action against the underlying infringers - the individual downloaders - more, it appears, as a sort of advertising campaign to stop P2P sharing than as a real means of obtaining compensation for lost revenues.

THE LAWSUITS

The causes of action for contributory and vicarious liability for copyright infringement discussed above presume an underlying infringement. That is, in order for the Napsters and Groksters of the world to be liable for copyright infringement, it must first be shown that "someone" was using their services to infringe on copyright.[25] In the suits against the service providers, no one seems to have really argued that the persons downloading the music were not infringing on copyrighted material. In the Napster case, in fact, the Court notes that, "'it is pretty much acknowledged … by Napster that this is infringement.'"[26] Napster did, however,

assert several defenses, based on "fair use", stating that the works were simply transformative, that file sharing actually raised, rather than lowered compact disc sales, that the users were simply "sampling" music prior to buying, that users were simply "space-shifting" the material from their CDs to their computers, and that users were simply using material for personal home use.[27] All of these arguments were readily dismissed by the Court, given the fact that the entire product was copied, the effect on the market for the original product, and the commercial nature of the use (the court found many benefits gained by users).[28] Although the underlying infringement was apparent, however, the record industry members did not pursue individual infringers initially. The Aimster Court gives a probable explanation:

> *The swappers, who are ignorant or more commonly disdainful of copyright and in any event discount the likelihood of being sued or prosecuted for copyright infringement, are the direct infringers. ... Recognizing the impracticability or futility of a copyright owner's suing a multitude of individual infringers ... the law allows a copyright holder to sue a contributor to the infringement instead.*[29]

The attempt to file lawsuits against individuals who use file-sharing software does appear to be a "futile crusade", one opponent noting that over 60 million such individuals existed in mid 2003.[30] With nowhere else to turn, however, the music industry has decided to indeed take this rocky road.

The impracticability of the matter does not seem to have detered the industry and, in fact, the random nature of the lawsuits against individuals seems to be an actual strategy. The President of the RIAA, Cary Sherman, has been quoted as saying "Lawsuits are an important part of the larger strategy to educate file sharers about the law, protect the rights of copyright owners and encourage music fans to turn to these legitimate services."[31] A September 30, 2004 press release found on the RIAA website again emphasizes the organization's position that the lawsuits against university network users are designed to "drive the message to students that unauthorized downloading has consequences" and to make students aware of legal alternatives.[32] Indeed, the industry has gone about this in a big way, filing thousands of lawsuits against individuals they claim illegally downloaded music or shared files. The suits began slowly in Spring 2003, with periodic headlines alerting the public about the potential for suit against individuals who were considered major infringers, for instance, running P2P networks on campus.[33]

The first major round of lawsuits with a broader scope of plaintiffs was filed in September 2003, and soon drew criticism for randomly attacking miniscule users, and even prompting Grokster president, Wayne Rosso, to compare the RIAA's actions to that of Stalin and McCarthy.[34] The RIAA CEO, however, stated that same month during Senate hearings that the industry was targeting only those "who are illegally distributing a substantial amount of copyrighted music."[35] At this time, the "John Doe" suit strategy, described below, appears to be in full-swing. The industry has filed suit and filed a corresponding press release every month since February 2004, like clockwork, indicating a new batch of hundreds of suits filed against individuals file-sharers.[36] Though clearly not limited to such cases, the most recent suits predominantly target college campuses.[37] Whether this targeting resulted naturally from the location of most downloads and was already the focus of suits or whether the RIAA is attempting to detract from bad publicity received for targeting 12 year olds and grandparents, the news releases since summer emphasize the campus target. No major campus seems to have gone unscathed, from Colorado to Massachusetts and from Oregon to Mississippi.[38] The RIAA has determined that it is up to them to train these college-aged customers in proper use of copyrighted material, and that the lawsuits "are an essential educational tool."[39] Whether these suits are accomplishing their goal or just causing ire among customers is what this survey and research address.

HOW WILL THEY FIND ME?

In order to sue an individual for copyright infringement, it seems logical that the RIAA would need to know who that person is. This, initially, was not a large issue for the industry. The DMCA provides for a "short-cut" subpoena whereby the copyright holder need only provide the ISP with notification of a claimed infringement, the identity of the copyrighted work and enough information to locate the material, the subpoena and a sworn statement that the information was sought for the purpose of enforcing copyright.[40] Most ISPs complied with the "§512" subpoenas. The RIAA, upon receipt of the information, sent warning letters to the individual users and filed lawsuits. Two major ISPs, however, decided to challenge the subpoenas on the basis that §512 does not apply to them because the subpoena provisions require the RIAA to identify material for the server to locate and remove or disable.[41] Where the more modern server is acting only as a "mere conduit" of information, and no caching or storage is involved, such a requirement cannot be met.[42] The court in RIAA v. Verizon agreed, rejecting the RIAA's argument that the

ISP could disable access simply by terminating the subscriber's internet account.[43] The District Court out of D.C., once again, tells the RIAA, shocked that the "agreed exchange" of a liability shield for ISPs for information has been breached, that their solution is with Congress and not the courts.[44] The ruling does not eliminate the ability of the RIAA to subpoena information from the ISPs, it merely eliminates the short-cut, requiring the industry to actually file a "John Doe" suit against the accused infringer and issue a regular "Rule 45" subpoena, allowable when a lawsuit is filed.[45] Filing a lawsuit is, obviously, much more expensive and burdensome to the industry, especially as an "ad" campaign, but has been adopted, as seen in the onslaught of "John Doe" suits. Potential defendants, at least in one area of the country, recently won some relief from potential suits when a Northern District of California Court ruled that "random joinder" by the Motion Picture Association of America (MPAA) of Doe defendants in lawsuits for purposes of obtaining subpoenas, while attempting to avoid filing fees, would not be permissible.[46] This should again raise costs for the industry pursuing infringers.

In addition to fighting the subpoenas based on conduit status, the servers have asserted that they violate the customer's free speech and "privacy" rights.[47] The privacy cry has become popular with the program developers and those seeking to make free P2P file-sharing legal, in a sort of "we're on your side" kind of way.[48] In the case of Sony v. Does 1-40 out of the federal trial court for the Southern District of New York, the industry sought information through subpoenas issued to Cablevision, the defendants' ISP. The court recognized that file-sharing, though not traditional "speech", is qualified for 1st Amendment protection under the broad scope given to freedom of speech and expression.[49] However, the constitutional rights of the defendants did not outweigh the "state's" need to enforce the law, where there was a prima facie case of infringement shown and the subpoena was necessary to pursue the case because the information was not available through other sources.[50] In addition, the court noted that the defendants would have minimal expectation of privacy in downloading and distributing copyrighted songs without permission.[51] In fact, the Verizon trial court had addressed this issue as well, stating that, "it is hard to understand just what privacy expectation [the file-sharer] has after essentially opening the computer to the world."[52] In short, where a "John Doe" suit has been filed and an IP address is provided to the ISP, the industry will be given the information necessary to locate and serve an accused individual infringer.

I GET SUED. SO WHAT?

Initially, there appears to be a conflict between general statistics and the opinions of individual students when asked about the effect of the lawsuits in stopping illegal file-sharing. The industry clearly believes the suits work, as noted in their various press releases. In addition, statistics have been cited indicating that the subpoenas alone have a stiffling effect on file sharing. Some show a drop of as much as 50% between Spring 2003 and the end of that year, with use of particular software down significantly as well – 15% for KaZaa and 59% for Grokster.[53] On the other hand, our survey suggests that the fact that the RIAA has the ability to sue an individual does not appear to have much of an effect on students, in general. Even students having a friend that had his network access cut off do not feel threatened. According to the student at Colorado State University, "My friends are like 'It won't happen to me."[54] The apparent discord may not be difficult to explain. At the Senate Hearings on the matter, experts addressed the issue of the effect of the lawsuits and presented the theory that, though the suits will act as a short-term deterrent, long-term effects are doubtful.[55] The industry's monthly filings indicate it recognizes the possibility that students have short-term memories, seemingly using a great amount of its advertising budget on filing fees. Additionally, some students may be demonstrating a general attitude of "invincibility" that comes with youth. The thought that no one would be interested in the few downloads they have made may contribute. After all, most would not place themselves in the category of someone who has illegally shared over 1000 copyrighted works.[56]

This was the presumption of Lorraine Sullivan – a full-time student with a part-time job - who, first, presumed KaZaa must be legal, since Napster had been shut down and, second, only downloaded music for "home, personal use" – a play list to listen to when cleaning house or doing homework.[57] On the contrary, however, Sullivan and many others did not understand the basic framework of the programs that leaves your file open to other sharers, unless you purposefully close it, giving accessibility to all downloaded files to anyone utilizing the program.[58] The Aimster Court explained, "the purchase of a single CD could be levered into the distribution within days or even hours of millions of identical, near-perfect copies … of the music recorded on the CD."[59] This is the approach the RIAA is taking, explaining how the 4 students originally sued in April 2003 could be liable for distribution of 27,000 files, 500,000 files, 650,000 files and over 1,000,000 files, respectively.[60] Sullivan, while not noting how many files were in her shared folder, was told that she would have to pay up to $150,000 for each such file by RIAA

attorneys, although she had already dismantled the KaZaa program she had used and deleted all files.[61] Sullivan settled with the industry for $2,500.[62] Other unsuspecting users felt the sting as well. The settlement of the RIAA with the mother of a 12-year-old Manhattan school girl accused of distributing more than 1000 songs claimed headlines in September 2003.[63] The girl's mother was on public assistance at the time, but managed to fork over $2000 to the RIAA with the aid of a special interest group.[64] These cases and others, such as the one against a 71-year-old grandfather in Texas and the one against the working mom whose teenage children downloaded music on their own computer unbeknownst to her, were the basis of objections to the RIAA's methods by Senators Norm Coleman (R-Minn.) and Susan M. Collins (R-MA).[65] As mentioned previously, they may well also be the reason the RIAA is focusing on college campus students who are less likely to garner such sympathy from strangers.

Though talk of taking on the RIAA is common, this is easier said than done when you are at the receiving end of a threatened lawsuit for millions of dollars. The tactics of the RIAA are aggressive, though not illegal. As explained by Sullivan, and presuming this was a typical procedure, as did the Senate Committee asking her to testify on the matter, she found out the RIAA sued her from news reporters. She had been notified of subpoenas for her information by her ISP, but had no further notice letters from the RIAA prior to the lawsuit.[66] Letters indicating warnings of potential lawsuits were apparently sent out in some cases, indicating what steps the prospective defendant should take to prevent suit and indicating that the RIAA will "assume you are not interested in settlement and proceed to litigation if we do not hear from you within ten (10) calendar days from the date of this letter."[67] In addition, the RIAA has contacted various institutes of higher education, obviously, as well as employers of alleged infringers, potentially affecting futures and careers of illegal downloaders.[68] She was told by lawyers for the RIAA, basically, that she could choose between facing a lawsuit for up to $150,000 dollars per file shared or sending the RIAA a couple of thousand dollars immediately.[69] Settlement is payable immediately by cashier's check, with no possibility of paying over time.[70] The mother of the 12 year old also began with a vow to fight the industry, only to settle the suit a day later.[71] In announcing the settlement with the mom of the 12-year-old, the RIAA CEO stated that the group was "trying to send a strong message that you are not anonymous when you participate in peer-to-peer file sharing and that the illegal distribution of copyrighted music has consequences."[72] Point taken. Sullivan sums it up, certainly, for all persons sued

by the RIAA on her website: "I'm scared and stressed and more than just a little bit angry."[73]

BITING BACK

Sullivan is not the only one angry. As mentioned above, the RIAA methods of enforcement were addressed during the Senate hearings that were supposed to be aimed, as far as the RIAA was concerned at stricter enforcement of copyright laws. Senator Coleman took to the media, stating that the RIAA tactics are too excessive and that we need not "club people to death to get people to understand that downloading is a problem."[74] Websites and special interest groups have been formed to combat the RIAA and make them out to be the bad guys.[75] The RIAA believes it is taking the "higher ground," stating that these fines are simply "expensive lessons" for downloaders to learn, and that the lawsuits are raising awareness. Their public relations strategy, however, draws their own business ethics into question, even cited as a "terror campaign", rather than that of the infringers and acts as an enabler to the software distributors - certainly not an intended consequence.[76]

Perhaps the most all-encompassing website dedicated to countering the RIAA efforts is the Electronic Frontier Foundation (EFF) site and the connected Subpoena Defense Alliance site.[77] Between the sites, nearly every lawsuit filed by or against the RIAA is included, with attached public documents, sample notice letters and challenge motions are provided as well as legal memoranda, potentially useable by accused parties, as well as a list of lawyers willing to represent defendants. In addition, the sites provide a list of "persons" the RIAA is seeking and advice on how not to be sued by the RIAA. In a world where civil defense does not come with appointed lawyers, access to justice does not come cheap, causing most defendants to settle the claims as urged by RIAA lawyers.[78] However, some defendants, certainly supported financially as well as emotionally by special interest groups are answering and challenging the industry. Early attempts by the RIAA to begin an amnesty program were met with harsh criticism and a lawsuit alleging that potential defendants would be led out of the closet with no real protection from legal action.[79]

One defendant has recently gone full force and effect in countering an RIAA lawsuit against her. Defendant Michelle Scimeca located a lawyer to take her case on contingency, implying more than an intent to simply state "I didn't do it."[80] Scimeca's answer and counterclaim, in addition to stating her basic defense, claim

many of the defenses utilized in the program cases, including fair use, invalid subpoena, privacy rights and various statutes, but also claim "laches", that, basically, defendants sat on their laurels and didn't do anything to prevent damage to themselves, fraud on the copyright office, misuse of copyright, collateral estoppel, illegality of copyrighted works based on immorality and libel, deceptive advertising, waiver, and RICO - that the industry conspired to file hundreds of frivolous suits in an effort to grab up financial settlements, amounting to "fear-inducing" extortion, mail and bank fraud.[81] The answer, appropriately so given the original purpose of RICO, paints the picture of an Al Pacino movie. More of the defendants will have the more subtle approach Sullivan says she will take - not buying any more CDs or anything else the industry puts out.[82]

AND NOW WHAT?

The Senate Committee on Governmental Affairs held hearings on potential solutions to the problem of balancing interests of the RIAA and consumers in September 2003, the same month the industry began to pursue individual lawsuits with great gravity.[83] The industry, at that time, put on its best argument for greater enforcement capabilities, in addition to advertising and the promotion of legal "pay per" download sites.[84] Others, including the Senators mentioned above, advocated for the advertising campaign and promotion of legal alternatives sans the harsh enforcement procedures against individuals.[85] Some, on the other hand, including the traditional P2P program distributors, seek a broader "revamping" of copyright law to allow for full utilization of current technology.[86] Allegations have been exchanged of "dinosaur" methods by one side and simply stealing by the other. Prior to and since the hearings, bills have flown about in Congress on both sides of the issue, some attempting to make significant file-sharing a federal crime, while others attempt to place greater guards on subpoena grants.[87] Both sides are advocated on their respective websites as well, with no apparent hint at giving in.[88]

SPRING 2005 UPDATE

On February 28th 2005 a news report surfaced indicating that music industry executives were considering raising the wholesale price of digital music downloads.[89] The wholesale price is thought to be about 65 cents per song, with songs retailing for 88 cents to 99 cents. The executives argued that the current

pricing scheme was only "introductory," and that music download sales in 2003 of $300 million showed the market was ripe for a price increase.

Sales in 2004 were triple what they were in 2003, with Apple's iPod accounting for 65% of that total. Total iPod sales since its release now surpass 250 million songs, with a peak of 1.25 million in one day.[90]

Ironically, a late 2004 CAIDA study says that while music download sales have been rising dramatically, illegal peer-to-peer file swapping has not declined during this period.[91] More recently, the RIAA announced 753 new lawsuits aimed at alleged illegal file sharers.[92] This continues their pattern of filing a new round of such suits monthly.

THE STUDY

A web survey that measured music downloading activity was developed and administered to online students at a medium-sized regional state university. The survey was announced to students in a variety of business courses including Consumer Behavior, E-Commerce, and Business Ethics. Students who participated did so of their own volition, thus rendering this a volunteer sample. The online survey can be viewed at http://houseofapps.com/emd/index.html. A total of 254 usable surveys were collected in 2004.

A variety of demographic variables were measured, including gender, age, class standing, computer ownership, and internet usage. Respondents were then asked to rate their level of agreement/disagreement with 14 attitudinal statements that measured their views on both illegal and legal music downloading, industry pricing, music sharing, and the threat of being sued. Summary results of the relevant variables in this portion of the study appear in Tables 1, 2, and 3. In Table 1, demographic variables V1 through V10 (excluding V9) were each collapsed into two groups. The mean scores of the attitudinal variables V17 through V30 were then compared for the two groups in each demographic variable. The number of respondents observed in each category appear in parentheses. (Rows that do not total 254 reflect missing values.)

ANALYSIS AND DISCUSSION

Demographic variables in some instances werecollapsed into two groups, while others were dichotomous by nature. This allowed for t-tests for independent means to be performed on the mean scores calculated for the attitudinal variables.

Collectively, the mean scores on the attitudinal measures (see Table 2) demonstrate that these college students feel there is little wrong in copying music illegally. They also feel the recording industry should not be chasing individuals who do copy music. While the sample feels that the price of CDs is too high, they do feel that the current price-per-song at legal download sites is fair.

Surprisingly, the sample felt that while the government will never be able to get control of this problem, the fear of being sued personally was a deterrent to illegal downloading.

Table 1

Variable	Group 1	Group 2
V1: Gender	Male (121)	Female (133)
V2: Age	Age 18-24 (146)	Age 25 and up (106)
V3: Class rank	Undergraduate (206)	Graduate (48)
V4: PC ownership	Own PC (234)	Do not own PC (18)
V5: Internet access	Internet service at home (225)	No internet service at home (28)
V6: CD burdner ownership	Own CD burner (182)	Do not own CD burner (72)
V7: iPod, etc., ownership	Own iPod, etc. (53)	Does not own iPod, etc. (199)
V8: Internet usage	<=5 hrs per week online (151)	>5 hrs per week online (103)
V10: CD purchases	Buys <5 CDs per year (176)	Buys 5 or more CDs per year 78)

More statistically meaningful results were found when t-tests were performed using the demographic variables with the attitudinal measures. Table 3 below summarizes the significant differences found in this analysis.

The most telling differences were noted when age and ownership of a CD burner are compared to the various means. Age (V2) produced 10 significant differences at p=0.05, while CD burner ownership produced 8 significant differences.

These results indicate that the traditional college students age group is much more likely to scoff at the ethics of illegal music sharing and the threat of being sued. Furthermore, owning a CD burner is akin to having license to steal.

Of perhaps greater interest is a horizontal analysis of V24, the fear of being sued. Looking across the table for this variable it becomes apparent that a profile emerges of the fearless music pirate: young, male, owns a CD burner, and is a heavy internet user.

The findings of this study indicate a general acceptance of music piracy among nearly all demographic groups represented, but that the practice is predominantly among those in the traditional college age group. Furthermore, men in this group are the most likely to engage in flagrant illegal copying and file sharing.

Table 2: Summary of attitudinal measures (Strongly Disagree =1 to Strongly Agree =5)

Variable	Mean
V17: It is morally wrong to copy CDs for friends	2.35
V18: It is morally wrong to download unauthorized music from the internet.	2.98
V19: The record industry should prosecute those who have downloaded songs illegally from the internet.	2.33
V20: Prices ranging from 88 cents to 99 cents per song download are fair for consumers.	3.24
V21: The retail price of CDs is about right.	2.37
V22: File-sharing sites emerged because the perceived value of CDs was too low in relation to the number of good songs on each CD.	3.37
V23: The government will eventually be able to put an end to illegal file sharing on the internet.	2.26
V24: The threat of being sued will keep me from illegally sharing files on the internet in the future.	3.23
V25: It is wrong for the record industry to make such a big deal about music piracy.	2.79
V26: The relative ease of downloading and/or burning CDs makes it too tempting for me to swap music illegally.	2.92
V27: Other people in my household/dorm have engaged in unauthorized file sharing and/or CD burning.	3.18
V28: People would burn fewer CDs and share fewer files if the retail price of CDs were not so high.	3.81
V29: It is OK to burn a "mix CD" of your favorite tunes to give to a friend.	3.76
V30: I resent the anti-copying features some record labels have started putting on their CDs.	3.07

Thus, while many people in this study are not likely to download music for fear of being sued, they do not have many negative feelings toward the practice. Furthermore, the perceived value of CDs in relation to their prices is not favorable, indicating at best an ambivalence toward buying product, and a willingness to look the other way when others are copying music.

While it may be comforting to the recording industry to pinpoint pirating to a fairly narrow demographic, it is likely to be equally disconcerting to know that, across the board, people don't see this as a major ethical issue.

Table 3: Summary of t-tests for significant difference of means
(* denotes p <=0.05)

Variable	V1	V2	V3	V4	V5	V6	V7	V8	V10
V17		*				*	*		
V18		*		*	*	*			
V19		*		*	*	*	*		
V20	*	*			*		*		
V21	*								
V22									
V23									
V24	*	*				*		*	
V25		*				*			
V26		*							
V27		*				*			
V28			*			*			
V29		*		*		*	*		
V30		*					*		

The fact that illegal music downloads are still high in number, while the number of legal downloads has reached 300 million, is also disconcerting. It demonstrates that there is still an active black market for music, one that is unlikely to go away any time soon. Furthermore, it is possible that if the recording industry raises its prices, it could stop a good thing (legal music downloads) dead in its tracks.

The current pricing structure, while "introductory" perhaps in the view of industry officials, has been successful in capturing a large market. It is undetermined at this point if those who are paying for their music are the same as those who currently (or perhaps formerly) downloaded music illegally. It is possible that the current legal music downloaders are a new market for music downloads in general.

But it is also possible that a price increase could drive these purchasers (who may be converts or new users) to illegal downloading instead. We contend that a price increase at this point is premature, and could be detrimental to an emerging business category. The prospect of continuing to file endless lawsuits against individuals, and given the lack of ability to pursue cases against the programmers, also does not seem appetizing.

The results reported above, coupled with the most recent industry data on legal and illegal downloads, suggest that consumers have not embraced the "legal" model of music downloads, and thus the emerging market for legal music downloads is tenuous at best. Thus, from a marketing standpoint, pricing should be held steady until there is a noticeable drop in the amount of illegal music downloads, for then the industry will have some assurance that there has been change in consumer behavior in attitude and practice.

LIMITATIONS AND FUTURE RESEARCH

The findings reported herein are not necessarily generalizable across the US population, given the narrow sample. Still, there is little reason to believe that students at this university vary much in outlook and practice from students at other universities. As evidenced by the RIAA lawsuits, wholesale music piracy appears to be an equal opportunity activity across US campuses. Still, a cross-sectional research project incorporating students at numerous universities would be an admirable extension of this research.

It would also be interesting to compare the findings in this study with industry data for CD sales broken down by the various age groups, as well as consumer data for legal music downloads that are purchased.

Still, the ubiquity of powerful PCs , and, more recently, portable devices such as iPods, have made music piracy a recreational activity. The industry has become an unwitting victim of technology proliferation, and it may matter little how low the price per song is on legal download sites. For as long as a person can copy music freely, the issue of ethics may be moot.

ENDNOTES

1 Statement of Mitch Bainwol, "Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry", Senate Committee on Governmental Affairs, September 30, 2003, available at http://www.senate.gov/~gov_affairs/index (hereinafter "Senate Hearings")

2 Id.

3 Statement of Susan M. Collins, Senate Hearings, supra

4 Id.

5 A&M Records, Inc., et. al. v. Napster, Inc., et. al., 239 F.3d 1004, 1025 (9th Cir. 2001), as amended April 3, 2004

6 A&M Records, Inc., et. al. v. Napster, Inc., et. al., 284 F.3d 1091, 1099 (9th Cir. 2002)

7 Id. at 1095

8 A&M Records, 239 F.3d at 1021

9 Id. at 1023

10 Id.

11 In Re: Aimster Copyright Litigation, 334 F.3d 643, 655 (7th Cir. 2003), cert. denied, Deep v. Recording Indus. Ass'n of Am., Inc., 124 S.Ct. 1069 (2004); Title II of the DMCA, 17 U.S.C. §512, also known as the Online Copyright Infringement Liability Limitation Act or OCILLA, provides for "safe harbors" for (1) transitory digital network communications, (2) system caching, (3) information residing on systems or networks at the direction of users and (4) information location tools, but only if the service provider has a policy for terminating network service to repeat offenders that it as informed users of and has reasonably implemented and the service provider accommodates and does not interfere with standard technical measures copyright owners use to identify and protect copyrighted works. Ellison v. America Online, Inc., 357 F.3d 1072, 1076-77, 1080 (9th Cir. 2004)(reversing summary judgment in favor of AOL in contributory and vicarious infringement of science fiction works by Ellison based on safe harbor defense and holding AOL

could be liable if safe harbor requirements not met); Canadian courts, on the other hand, have continued to reaffirm ISPs as neutral conduits with no liability for infringement, even if a cache is involved. "Highest Canadian court decides that ISPs do not owe royalties on downloaded music",International Law Update, Vol. 10, No. 7 (July 2004) (Transnational Law Associates, LLC 2004).

12 Id. at 655. The Aimster Court, having found contributory infringement, did not find it necessary to address vicarious liability. Id. at 653.

13 Metro-Goldwyn-Mayer Studios, Inc., et. al. v. Grokster, Ltd., et. al., 380 F.3d 1154, 1159 (9th Cir. 2004). The "Grokster" suit was brought by almost every motion picture studio and recording company and by approximately 27,000 songwriters and publishers. Id. at n. 1

14 Id.

15 A&M Records, 239 F.3d at 1011

16 MGM, 380 F.3d at 1159

17 Id.

18 Id. at 1154

19 Id. at 1163

20 Id. at 1161; The concept that if a product used for copyright infringement has substantial non-infringing uses, contributory negligence will not necessarily be found, had been established many years before in the case of Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984), generally known as the "Betamax case", involving whether VCR producers were liable for contributory copyright infringement.

21 Id.

22 Id. at 1166

23 Id. at 1167 (citing Sony, 464 U.S. at 456)

24 Zeller Jr., Tom, " Entertainment Industry Asks Justices to Rule on File Sharing," N.Y. Times (10/24/04) (quoting the music industry's Petition for Writ of Certiorari);

"Unprecedented Coalition of Creators, State Attorney Generals, Digital Entertainment Services and Academics ask Supreme Court to Review File-Sharing Decision," Press Room, RIAA Website at http://www.riaa.com/news/newsletter/111804.asp. (RIAA 2004); see also MGM cite, supra.

25 A&M Records, 239 F.3d at n.2

26 Id. at 1014, quoting the district court opinion; the Grokster Court simply states that the question of direct infringement is not an issue in the case. MGM, 380 F.3d at 1160

27 Id. at 1014 – 1019

28 Id. at 1019

29 In re Aimster, 334 F.3d at 645

30 "How to Tell if the RIAA Wants You", Wired News at http://www.wired.com/news/digiwood/0,1412,59785,00.html (April 16, 2003), quoting Fred Von Lohmann, senior attorney with the Electronic Frontier Foundation.

31 Martin, Anna, "New Wave of RIAA Lawsuits to Target Students", Technician at technicianonline.com/04.07.2204/news/ (North Carolina State University SMA 2004)

32 "RIAA Brings Lawsuits Against 762 Illegal File Sharers", RIAA Website at http://www.riaa.com/news/newsletter/093004.asp (RIAA 2004)

33 Dean, Katie, "RIAA Hits Students Where It Hurts", Wired News at http://www.wired.com/news/digiwood/0,1412,58351,00.html (April 5, 2003); See also, Statement of Mitch Bainwol, Senate Hearings, supra.

34 Losi, Stephanie, "RIAA Sues Hundreds in 'First Wave' of War", Ecommerce Times News Network (September 8, 2003), http//www.technewsworld.com/perl/story/31525.html; Dean, Katie, "RIAA Legal Landslide Begins", Wired News at http://www.wired.com/news/print/0,1294,60345,00.html; Mello, Jr., John P., "RIAA Settles First Lawsuit Against 12-Year-Old Brianna LaHara", TechNewsWorld at http://www.technewsworld.com/perl/story/31561.html (9/11/03)

35 Statement of Mitch Bainwol, Senate Hearings, supra. (indicating individuals sued averaged 1000 music files made available to others); see also, Statements of Senator Susan M. Collins, Senator Norm Coleman, Senate Hearings, Supra, indicating concern over the RIAA tactics and unintended potentially harsh consequences on some defendants; see also, press release of Senator Coleman, "Coleman Concerned Recording Industry's Rubber-Stamp Subpoenas Inadvertently Target Unwary Consumers: 'Law of Unintended Consequences' May Be Needlessly Threatening American Citizens", http://govt-aff.senate.gov/index

36 See Press Releases dated 2/17/04, 3/23/04, 4/28/04, 5/24/04, 6/22/04, 7/20/04, 8/25/04, 9/30/04, 10/28/04 and 11/18/04, each indicating a new set of lawsuits and sporting similar titles to the 3/23/04 release: "RIAA Brings New Round of Cases Against Illegal File Sharers", RIAA website, supra, http://www.riaa.com/news/newsletter (The site was accessed 12/03/04 - too early for the next round. It remains to be seen whether the industry will take a holiday break or whether file-sharers will receive subpoenas for Christmas.); see also list of "John Doe" suits found on the Electronic Frontier Foundation (EFF) website at http://www.eff.org/IP/P2P/?f=riaa-v-thepeople.html. The suits make good on the RIAA's promise following the initial September 2003 John Doe suits that further legal action would follow. Lyman, supra. Groups in other countries have joined the front line on this fight against P2P file sharing as well. See, for example, "Music Industry Calls Time on Illegal Downloading", Swissinfo at http://www.swissinfo.org/sen/swissinfo.html?siteSect=105&sid=4862096 (4/13/04); Arthur, Charles, "Record Bosses Sue for Downloading of Songs", The Independent (London), October 18, 2004 (2004 Newspaper Publishing PLC)

37 See RIAA Press Releases, supra.

38 Id.; Huseby, Josh, "Entertainment: The Dish Live - The RIAA Targets Colorado Campuses", The Rocky Mountain Collegian.com of Colorado State University at http://www.collegian.com/vnews/display.v/ART/2004/04/01/406ba75e8082d (April 1, 2004)

39 "Illegal File Sharing Targeted in Wave of New Lawsuits", Press Room, RIAA website, supra. (11/18/04). It is also noted that the RIAA also works with various colleges and universities in enforcement and encourages the institutions of higher education to enter into agreements with legal file-sharing sites. Id. In fact, a Joint Committee of the Higher Education and Entertainment Communities was appointed to review the matter of file-sharing on campus and recently issued its report to Congress. "Universities, Entertainment Industry Leaders Issue Report to Congress on Latest Efforts to Curb Illegal File Sharing on College Campuses, [CITE] August

24, 2004; Dean, Katie, "RIAA, Colleges Seek Piracy Fix", Wired News at http://www.wired.com/news/digiwood/0,1412,59743,00.html (July 25, 2003)

40 RIAA, Inc., v. Verizon Internet Services, Inc., 351 F.3d 1229, 1232 (2003), as amended January 16, 2004, cert. denied, 2004 U.S. LEXIS 6700 (2004) and by 2004 U.S. LEXIS 6701 (2004), citing the DMCA, 17 U.S.C. § 512(h); SBC, the other major ISP rejecting the subpoenas, took a different route and filed for declaratory relief against the RIAA. McMillan, Robert, IDG News Service, "Judge Considers Pacific Bell, RIAA Case - ISP hopes to protect names of 200 customers accused of file sharing", PCWorld at http://www.pcworld.com/news/article/0%2Caid%2C113641%2C00.asp (11/24/03)

41 Id. at 1234-35

42 Id.

43 Id. at 1235-36

44 Id. at 1236; See also, Statement of Mitch Bainwol, Senate Hearings, supra, regarding the industry's position that the DMCA exemptions from liability were a "trade-off" for disclosure of information necessary to pursue infringers.

45 Subpoena Defense Alliance website at http://www.subpoenadefense.org/index.htm (citing and attaching the court order from Elektra Entertainment Group, Inc. v. Does 1-6 out of the Eastern District of Pennsylvania and dated 10/13/04; the IRAA argues that the ISPs involved are not attempting to protect identities of customers, but are, in fact, protecting their own future DSL earnings. Mr. Bainwol points out that where information is obtained in a §512 subpoena, it is protected from disclosure outside of the stated use, but information obtained from a lawsuit subpoena is not. Statement of Mitch Bainwol, Senate Hearings, supra

46 "Court Blocks Movie Studios' Bulldozer Legal Strategy", EFF, supra at http://www.eff.org/news/

47 Sony Music Entertainment, Inc. v. Does 1-40, 326 F. Supp. 2d 556, 558 (S.D. N.Y. 2004)

48 Statement of Alan Morris, Executive Vice President of Sharman Networks Limited (KaZaa), Senate Hearings, supra; Lyman, Jay, "RIAA Showdown Set, FCC Rules Blasted", TechNewsWorld at http://www.technewsworld.com/perl/story/31585.html

(9/15/03)(noting the EFF filed a supporting brief on behalf of about 45 consumer privacy, civil liberty and ISP associations in the Verizon appeal)

49 Id. at 564.

50 Id. The industry would argue that the constitutional rights of the copyright holders were violated, copyright being a direct result of powers given in the constitution to protect creative works, by the lack of ability to quickly gain access to infringers information where continual infringement would be an issue. Statement of Mitch Bainwol, Senate Hearings, supra.

51 Id. at 566

52 Id. at 567 (citing In re Verizon Internet Servs., Inc., 257 F. Supp 2d 244, 267 (D. D.C. 2003), rev'd on other grounds, RIAA v. Verizon, 351 F.3d at 1229)

53 Cox, Evan R., "RIAA Resumes Legal Offensive: Recording Industry Association Uses John Doe Lawsuits Against P2P File-Swapping Post-Verizon", Internet Newsletter, January 28, 2004 (ALM 2004) and "Jailing Joe College", Editorial, St. Louis Post-Dispatch, September 20, 2004 (both citing study conducted of 1300 internet users from November 18 – December 14, 2003, by Pew Internet & American Life Project, www.pewinternet.org)

53 Cox, Evan R., "RIAA Resumes Legal Offensive: Recording Industry Association Uses John Doe Lawsuits Against P2P File-Swapping Post-Verizon", Internet Newsletter, January 28, 2004 (ALM 2004) and "Jailing Joe College", Editorial, St. Louis Post-Dispatch, September 20, 2004 (both citing study conducted of 1300 internet users from November 18 – December 14, 2003, by Pew Internet & American Life Project, www.pewinternet.org)

54 Huseby, supra.

55 Statement of Jonathan D. Moreno, PhD, Director , Center for Biomedical Ethics, University of Virginia, Charlottesville, Senate Hearings, supra; See also, Statement of James V. DeLong, Senior Fellow & Director, Center for the Study of Digital Property, The Progress & Freedom foundation, Senate Hearings, supra (discouraging "quick fixes" by Congress in addressing problem of illegal file-sharing)

56 See, Statement of Mitch Bainwol, Senate Hearings, supra (noting that lawsuits targeted infringers who averaged distribution of 1000 copyrighted recordings)

57 Testimony of Lorraine Sullivan, Senate Hearings, supra; see also, Sullivan's website to raise money to cover costs of her settlement, "Sued By The RIAA" at http://www.suedbytheriaa.com/ (accessed 4/16/04)

58 Sullivan website, supra (Noting, "As far as opening my 'shared folder' I didn't even know I was doing it. I'd installed p2p software and it went automatically to a folder which stored the songs I'd downloaded.")

59 Aimster, 334 F.3d at 646

60 Dean, "RIAA Hits Students", supra

61 Statement of Lorraine Sullivan, Senate Hearings, supra

62 Id.

63 Dean, Katie, "Schoolgirl Settles With RIAA", Wired News at http://www.wired.com/ news/digiwood/0,1412,60366,00.html (9/10/03)

64 Id.; Statement of Lorraine Sullivan, Senate Hearings, supra (indicating RIAA attorney told her that she would not be able to settle for as low an amount as the school-girl's mom, because the mom was on public assistance); Mello, supra.

65 Dean, "Schoolgirl Settles", supra; Statements of Norm Coleman and Susan M. Collins, Senate Hearings, supra.

66 A Pennsylvania Federal District Court recently ruled that it would require notice of the subpoenas be given to potential defendants when information was sought from the ISP, in order that the individual could take steps to challenge the subpoena prior to the time the information was given out. See, Subpoena Defense Alliance, supra, citing Elecktra v. Does 1-6.

67 Electronic Frontier Foundation at http://www.eff.org, supra, attaching a copy of Sample Recording Industry Letter Threatening to File a Lawsuit. Interestingly, while attorneys apparently told Sullivan and others to destroy all illegal files and this is part of the Doe Settlement Form, infra, the notice letter specifically warns that destruction of such evidence could lead to severe legal consequences.

68 McCausland, Margaret A. and Jennifer J. Platzkere, "Warning! Employee's Entertainment May Be Employer's Headache", The Corporate Counselor, Vol. 18, No. 11, p.1 (Feb. 2004)

69 Statement of Lorraine Sullivan, Senate Hearings, supra.

70 Id.; Doe Settlement Agreement Form, accessed from Electronic Frontier Foundation at http://www.eff.org/IP/P2P/?f=riaa-v-thepeople.html

71 Dean, "Schoolgirl Settles", supra; Mello, supra

72 Mello, supra.

73 Sullivan website, supra

74 Dean, "Schoolgirl Settles", supra

75 See http://www.boycott-riaa.com/; Crawford, Michael D., "Links to Tens of Thousands of Legal Music Downloads", GoingWare, Inc. at http://www.goingware.com/tips/legal-downloads.html. The article is an eclectic mix of topics, at one instance dedicated to drawing support from independent artists for the proposal to bypass the record industry and market directly from P2P networks, not charging for licensing, but potentially benefiting from other sales, and at another, calling for the complete dismissal of copyright law; Sandburg, Brenda, "File Sharing Seeks Special-Interest Status", The Recorder (2004 ALM Properties)

76 Mello, supra, quoting Adam Eisgrau of P2P United, who calls the RIAAs suits, including that against the 12-year-old, a "legally suspect and morally reprehensible … terror campaign."

77 Electronic Frontier Foundation, supra; Subpoena Defense Alliance, supra.

78 Initial lawsuits against students running sites for downloaders settled for between $12,500 and $17,000. Statement of Mitch Bainwol, Senate Hearings, supra. Most of the individual lawsuits appear to have been settled in the range of $3,000, according to one student writer. Huseby, supra.

79 Cassavoy, Liane, "Consumers Strike Back, Sue RIAA - 'Deceptive' Amnesty Program Puts Participants at Risk, Lawsuit Claims", PCWorld.com at http://www.pcworld.com/resource/printable/article/0,aid,112428,00.asp (9/11/03); Dean, Katie, "Lawsuit Attacks RIAA Amnesty Plan", Wired News at http://www.wired.com/news/print/0,1294,60376,00.html

80 Fineman, Samuel, "Record Industry Still Pursuing File Sharers - One Alleged Abuser Fights Back in Court", The Internet Newsletter, March 9, 2004 (2004 ALM Properties)

81 See, Answer to Complaint (1/14/04) and Counterclaim (2/04/04) filed in Sony Music v. Michele Scimeca, accessible from through EFF website, supra. Although not apparent from the answer and counterclaim, Scimeca may attempt to revamp antitrust violation allegations, last seen in the Napster trial court on remand, under the listed defense of "misuse of copyright." In re Napster, 2004 U.S. Dist. LEXIS 7236 at p. 56-57 (N.D. Cal. 2004)

82 Statement of Lorraine Sullivan, Senate Hearings, supra

83 Senate proceedings and transcripts are available at http://www.senate.gov/~gov_affairs

84 See, Statements of Mitch Bainwol, Jack Valenti, head of the MPAA, Chris Gladwin, owner of a "pay per" site, Senate Hearings, supra.

85 See, Statements of Susan Collins, Lorraine Sullivan and Norm Coleman, Senate Hearings, supra.

86 Statement of Alan Morris, Senate Hearings, infra

87 See, "Jailing Joe College", supra (Editorial: House Committee approves bill making file sharing a federal crime; "…college dormitory will contain more criminals than the county jail."); Proposed Author, Consumer and Computer Owner Protection and Security Act of 2003 (ACCOPS) (as indicated above, for enforcement); Proposed Piracy and Deterrence Education Act of 2003 (to enhance copyright laws and provide more power for enforcement); Proposed Consumers, Schools and Libraries Digital Rights Management Awareness Act of 2003 (requiring a John Does suit to be filed for a subpoena)

88 See, for instance, EFF site and Boycott-RIAA site, supra; RIAA site, supra.

89 http://money.cnn.com/2005/02/28/technology/personaltech/music_downloads/index.htm?cnn=yes

90 http://news.com.com/iTunes+hits+250+million+downloads/2110-1027_3-5547939.html

91 "Is P2P Dying or Just Hiding?" Karagiannis, Thomas, at al (2004), http://www.caida.org/outreach/papers/2004/p2p-dying/p2p-dying.pdf

92 "Copyright Infringement Lawsuits Brought Against 753 Additional Illegal File Sharers," (Feb 28, 2005), http://www.pcpro.co.uk/news/69951/riaa-fires-off-fresh-suits-against-filesharers.html

REFERENCES

A&M Records, 239 F.3d at 1011

A&M Records, 239 F.3d at 1021

A&M Records, Inc., et. al. v. Napster, Inc., et. al., 284 F.3d 1091, 1099 (9th Cir. 2002)

A&M Records, Inc., et. al. v. Napster, Inc., et. al., 239 F.3d 1004, 1025 (9th Cir. 2001), as amended April 3, 2004

Aimster Copyright Litigation, 334 F.3d 643, 655 (7th Cir. 2003), cert. denied, Deep v. Recording Indus. Ass'n of Am., Inc., 124 S.Ct. 1069 (2004); Title II of the DMCA, 17

Cassavoy, Liane, (2003). "Consumers Strike Back, Sue RIAA - 'Deceptive' Amnesty Program Puts Participants at Risk, Lawsuit Claims", PCWorld.com at http://www.pcworld.com/resource/printable/article/0,aid,112428,00.asp (9/11/03);

Dean, Katie, "Lawsuit Attacks RIAA Amnesty Plan", Wired News at http://www.wired.com/news/print/0,1294,60376,00.html

Cox, Evan R. (2004). "RIAA Resumes Legal Offensive: Recording Industry Association Uses John Doe Lawsuits Against P2P File-Swapping Post-Verizon", Internet Newsletter, January 28, 2004 (ALM 2004) and "Jailing Joe College", Editorial, St.

Louis Post-Dispatch, September 20, 2004 (both citing study conducted of 1300 internet users from November 18 – December 14, 2003, by Pew Internet & American Life Project, www.pewinternet.org)

Dean, Katie, (2004). "RIAA, Colleges Seek Piracy Fix", Wired News at http://www.wired.com/news/digiwood/0,1412,59743,00.html (July 25, 2003) August 24, 2004

Dean, Katie, (2003). "RIAA Hits Students Where It Hurts", Wired News at http://www.wired.com/news/digiwood/0,1412,58351,00.html (April 5, 2003); See also, Statement of Mitch Bainwol, Senate Hearings, supra.

Fineman, Samuel, (2004). "Record Industry Still Pursuing File Sharers - One Alleged Abuser Fights Back in Court", The Internet Newsletter, March 9, 2004 (2004 ALM Properties)

"How to Tell if the RIAA Wants You", (2003). Wired News at http://www.wired.com/news/digiwood/0,1412,59785,00.html (April 16, 2003), quoting Fred Von Lohmann, senior attorney with the Electronic Frontier Foundation.

Losi, Stephanie, (2003). "RIAA Sues Hundreds in 'First Wave' of War", Ecommerce Times News Network (September 8, 2003), http//www.technewsworld.com/perl/story/31525.html; Dean, Katie, "RIAA Legal Landslide Begins", Wired News at http://www.wired.com/news/print/0,1294,60345,00.html;

Mello, Jr., John P., "RIAA Settles First Lawsuit Against 12-Year-Old Brianna LaHara", TechNewsWorld at http://www.technewsworld.com/perl/story/31561.html (9/11/03)

Martin, Anna, (2004). "New Wave of RIAA Lawsuits to Target Students", Technician at technicianonline.com/04.07.2204/news/ (North Carolina State University SMA 2004)

McCausland, Margaret A. and Jennifer J. Platzkere, (2004)."Warning! Employee's Entertainment May Be Employer's Headache", The Corporate Counselor, Vol. 18, No. 11, p.1 (Feb. 2004)

Mello, supra, quoting Adam Eisgrau of P2P United, who calls the RIAAs suits, including that against the 12-year-old, a "legally suspect and morally reprehensible … terror campaign."

Metro-Goldwyn-Mayer Studios, Inc., et. al. v. Grokster, Ltd., et. al., 380 F.3d 1154, 1159 (9th Cir. 2004).

MGM, 380 F.3d at 1159

"RIAA Brings Lawsuits Against 762 Illegal File Sharers", RIAA Website at http://www.riaa.com/news/newsletter/093004.asp (RIAA 2004)

RIAA, Inc., v. Verizon Internet Services, Inc., 351 F.3d 1229, 1232 (2003), as amended January 16, 2004, cert. denied, 2004 U.S. LEXIS 6700 (2004) and by 2004 U.S. LEXIS 6701 (2004), citing the DMCA, 17 U.S.C. § 512(h);

Sony Music Entertainment, Inc. v. Does 1-40, 326 F. Supp. 2d 556, 558 (S.D. N.Y. 2004)

Statement of Alan Morris, Executive Vice President of Sharman Networks Limited (KaZaa), Senate Hearings, supra; Lyman, Jay, "RIAA Showdown Set, FCC Rules Blasted", TechNewsWorld at http://www.technewsworld.com/perl/story/31585.html (9/15/03)

Statement of Jonathan D. Moreno, PhD, Director , Center for Biomedical Ethics, University of Virginia, Charlottesville, Senate Hearings,

Statement of Mitch Bainwol, (2003). "Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry", Senate Committee on Governmental Affairs, September 30, 2003, available at http://www.senate.gov/~gov_affairs/index (hereinafter "Senate Hearings")

Statement of Susan M. Collins, (2003). "Privacy & Piracy: The Paradox of Illegal File Sharing on Peer-to-Peer Networks and the Impact of Technology on the Entertainment Industry", Senate Committee on Governmental Affairs, September 30, 2003, available at http://www.senate.gov/~gov_affairs/index (hereinafter "Senate Hearings")

Testimony of Lorraine Sullivan, Senate Hearings, supra; see also, Sullivan's website to raise money to cover costs of her settlement, "Sued By The RIAA" at http://www.suedbytheriaa.com/ (accessed 4/16/04)

Zeller Jr., Tom, " Entertainment Industry Asks Justices to Rule on File Sharing," N.Y. Times (10/24/04)

THE ROLE OF INTERNET-BASED TRANSACTIONS IN EXTERNAL COLLABORATION BETWEEN HEALTHCARE TRADING PARTNERS

Sang Man Kim, Kyung Hee University
Arben Asllani, University of Tennessee at Chattanooga
Lawrence Ettkin, University of Tennessee at Chattanooga

ABSTRACT

Increased collaboration between trading partners is a precondition for a successful performance of a supply chain. This paper investigates whether the Internet technology improves the level of collaboration between sellers and buyers, a dyad relationship, in a healthcare supply chain. Such collaboration is determined by the amount of information sharing and operational participation between these healthcare trading partners.

Among other statistical methods, structural equation modeling is employed to analyze the collected data (N=106) from a survey of hospitals, pharmacies, pharmaceutical companies, and healthcare equipment and supply retailers in South Korea. The results indicate that Internet-based transactions lead to a significant increase in information sharing, collaborative planning and forecasting, which are important indicators of supply chain performance.

INTRODUCTION

Today, electronic commerce has become a major competitive weapon in reducing cost, improving efficiency, and increasing customer satisfaction. Just in the healthcare industry alone, $336 billion worth of business to business (B2B) Internet-based transactions took place in 2000 and Forrester Research predicts that Internet-based transactions will increase to $6 trillion by the year 2005 (Standifer & Wall, 2003). In this environment, supply chain management may provide a considerable

source of opportunity for improving the efficiency of organizations (Layden, 1996). Like other industries, healthcare can benefit from a successful incorporation of the Internet into its supply chain management activities. Studies have shown that 30%-46% of hospital expenses are allocated into various stages of logistical activities, and that the costs associated with the supply chain process could be reduced by almost 50% through the use of best practices (Poulin, 2003). Efficient Healthcare Consumer Response (EHCR) estimates that "the healthcare products industry could significantly improve its ability to deliver quality healthcare products and services to consumers" (Arbietman, Lirov, Lirov & Lirov, 2001).

A majority of hospitals and other healthcare centers still utilize fax and telephone communication as the primary or the secondary methods for their purchasing activity, even though they possess a strong knowledge and capability in information technology. Their reliance on these traditional means of communication may result in poor planning and many rush orders, which can lead to higher delivery charges and increased costs for the items ordered. Usually, fax and telephone ordering typically "falls outside" of what should be a smooth process designed to handle most supply situations.

As the literature suggests, managers can improve coordination by increasing the accuracy of information available at different stages in the supply chain (Chopra & Meindl, 2004, p. 487). Information accuracy can be achieved through better information sharing, more collaborative planning and forecasting. The objective of this research is to empirically examine the role of Internet-based transactions in information sharing and external collaboration in the area of supply chain management.

With the increasing concerns for healthcare cost containment and service quality improvement, it is important to develop a framework that indicates the impact of B2B Internet-based transactions in supply chain performance in general and its cost in particular. This paper is structured as follows: First, we provide a brief discussion of previous literature on healthcare supply chain management and the implementation of Internet-based transactions in this service sector. Based on this review, we develop a framework, which represents the impact of B2B Internet-based transactions in the level of external collaboration between healthcare trading partners. After discussing our method and the study's results, we finish the paper with a discussion of the data and our conclusions.

PREVIOUS RESEARCH

Supply Chain Management (SCM) is broadly defined as the coordination of activities of the companies involved in producing, maintaining, and delivering products and services to customers, who are located in geographically different places (Viswandadham & Raghavan, 2000). SCM is more than just order fulfillment and encompasses all the process from product creation through end-of life recycling. These activities involve product design, introduction, promotion, fulfillment, recycling, and disposal (Kopczak & Johnson, 2003).

Real-time information sharing allows the suppliers to anticipate changing expectations and quickly update their entire organization on the new demands, which essentially leads to improving responsiveness, reduction in costs, and reducing uncertainty for the supply chain processes (Closs & Savitskie, 2003). As a result, supply chain success is heavily dependent on the efficiency and effectiveness of information exchange (Closs & Savitskie, 2003).

Researchers have also pointed out that integration of the supply chain in a collaborative manner between the customer and the supplier is an essential characteristic in achieving the objectives of supply chain management (Maloni & Benson, 1997; Simatupang & Sridharan, 2002; Kopczac & Johnson, 2003). A collaborative supply chain in which two or more independent organizations work jointly, leads to greater success in supply chain operation than one organization acting in isolation (Simatupang & Sridharan, 2002).

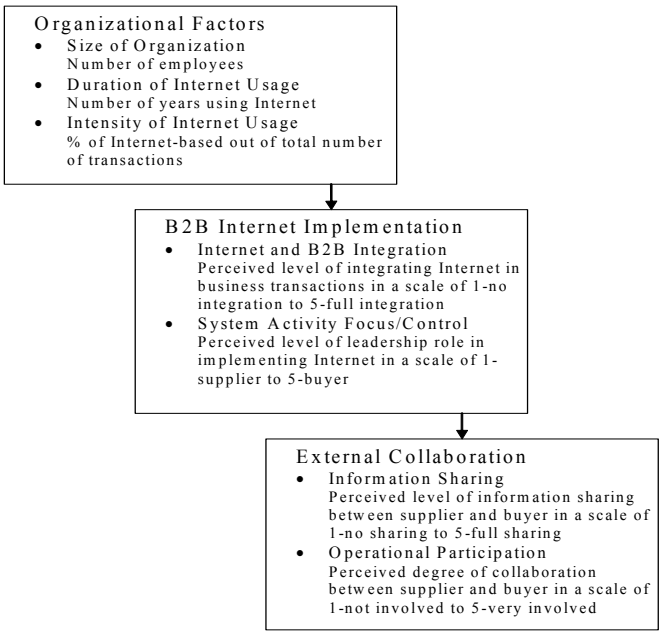
The Internet provides significant opportunities for organizations to establish distinctive strategic positions than did previous generations of information technology (Porter, 2001). According to Ghosh (1998), the Internet provides organizations the ability to build interactive relationships with customers and suppliers, and deliver products and services at very low costs. In fact, both suppliers and buyers benefit from an increased use of the Internet for their purchasing activities (Deeter-Schmelz, Bizzari, Graham & Howdyshell, 2001). Other major benefits from Internet-based transactions implementation would be rapid data exchange, lower inventory cost, and quick response to the customers' changing requirements (Archer & Yuan, 2000; Crouch, 2003). Because of such advantages, healthcare organizations have gradually moved from traditional communication systems into Internet-based supply chain management systems.

RESEARCH MODEL

Two major research questions are addressed in this study: First, we explore whether there is a relationship between several organizational factors and the level of integration of the Internet in B2B transactions. Secondly, we investigate whether there is a relationship between the level of Internet usage for B2B transactions and the level of external collaboration between selling and buying healthcare organizations. An overview of the research factors is presented in Figure 1.

In this context, three organizational factors will be analyzed: size of the organization, duration of Internet usage, and intensity of Internet usage. The size of the organization is measured by the number of employees in the firm. The duration of Internet usage represents how long the organization has been using Internet for electronic transactions. The intensity of Internet usage indicates the proportion of the Internet-based transactions in the supply chain that the organization uses out of its entire supply chain transactions.

Figure 1 Overview of Research Factors



RESEARCH METHODOLOGY

A survey was conducted among healthcare organizations located throughout South Korea. South Korea is a world leader in information and communication technology. The Organization for Economic Cooperation and Development (OECD) considers Korea as the world leader in high-speed Internet technology and recommended Korea as the model for benchmarking (Lee, 2003). Besides being a leading country in information and communication technology, Korea has recognized the need for improvement in supply chain effectiveness and the necessity of adapting to the new business environment. By 2006, business online connections are expected to be 100% and business electronic transactions are expected to reach 30%. Business-to-business network in Korea will be expanded to 50 industries by 2006 from 20 industries in 2001.

The initial questionnaire was developed in English, then it was translated into Korean, and finally it was translated back into English to ascertain the accuracy of the items in the questionnaire. The final version of the instrument is presented in Appendix A. The sample was drawn from 786 organizations in healthcare industry, which included hospitals, pharmacies, pharmaceutical companies, and healthcare equipments and supply retailers. The survey was conducted in the healthcare organizations throughout South Korea. Those samples were selected from the lists of Korean Hospital Association (KHA), Korean Medical Association (KMA), Korea Medical Devices Industry Association (KMDIA), and Korea Pharmaceutical Manufacturer Association (KPMA). Questionnaires were sent mostly to the director or vice president of the marketing department or operations department. For small sized organizations, the questionnaires were sent to the president or vice president.

Among the total of 786 questionnaires mailed, 142 were returned (18.01% returned response rate). Of those 142 returned questionnaires 36 of them were not usable because they were not answered completely nor did they indicate any usage of B2B Internet-based transactions. For the analysis, 106 subjects (13.48% usage returned rate) were used from the mail survey. Although the questionnaires were sent to the director or vice president of marketing or operations department, the respondents indicate other positions, such as presidents, managers, and staff. Tables 1, 2, and 3 indicate major demographics of the pool of respondents and their organizations. The descriptive statistics of the duration of Internet-based transactions implementation and intensity of Internet-based transactions usage are presented in Tables 4 and 5.

Table 1: Organizational Position of Respondents		
Position	Number of Respondents	Percentage
Presidents	5	4.72%
Directors	29	27.36%
Vice-directors	17	16.04%
Managers	28	26.42%
Staff	27	25.47%
Total	106	100.00%

Table 2: Size of Surveyed Organizations		
Number of Employees	Number of Organizations	Percentage
Less than 49	26	24.53%
50-99	14	13.21%
100-499	30	28.30%
500-999	21	19.81%
1000 or more	15	14.15%
Total	106	100.00%

Table 3: Type of Surveyed Organizations		
Type	Number of Organizations	Percentage
Hospitals	64	60.38%
Equipment and Supply Retailers	23	21.70%
Pharmaceutical Companies	11	10.38%
Pharmacies	8	7.55%
Total	106	100.00%

Table 4: Duration of the Internet Usage		
Duration	Number of Organizations	Percentage
Less than 1 year	20	18.87%
1 year to 2 years	29	27.36%
2 years to 3 years	31	29.25%
3 years to 4 years	15	14.15%
5 years and more	11	10.38%
Total	106	100.00%

Table 5: Intensity of Internet Usage		
Intensity of Usage	Number of Organizations	Percentage
Less than 10%	6	5.66%
10% to 19%	30	28.30%
20% to 29%	34	32.08%
30% to 39%	17	16.04%
40% to 49%	9	8.49%
50% and more	10	9.43%
Total	106	100.00%

RELIABILITY AND VALIDITY ANALYSIS

Reliability is defined as "a measure of internal consistency of the construct indicators, depicting the degree of which they indicate the common latent construct" (Hair, Anderson, Tatham, & Black, 1995). For instance, if reliability is high, the measurement gives the same results every time the same property is measured in the same way (Reaves, 1992). The results of reliability test for the Internet-B2B Integration and External Collaboration are presented in Table 6. The Cronbach's alpha is used as a reliability measure, and its values are respectively 0.6472 and 0.9267. While external collaboration is a reliable measure in our study, Internet-

based transactions integration has a reliability measure of 0.6472, which is lower than the suggested lower limit (0.7). However, considering the exploratory nature of this study this value will be considered acceptable.

Validity is defined as "the extent to which the indicators accurately measure what they are supposed to measure" (Hair, Anderson, Tatham, & Black, 1995). There are several procedures to assess validity of a measure: content, criterion, and construct validity. In this research, construct validity is employed. The purpose of construct validity is to assess the quality of correspondence between a theoretical construct and its operational measures (Babbies, 1995). The most widely used method to test construct validity is factor analysis. Factor analysis is concerned with exploring the patterns of relationships among a number of variables (Hair, Anderson, Tatham, & Black, 1995). These constructs include Organizational Factors, B2B-Internet Implementation, and External Collaboration.

Table 6: Reliability Test

Constructs	Number of Items	Alpha Value
Internet-B2B Implementation	2*	0.6472
External Collaboration	3**	0.9267

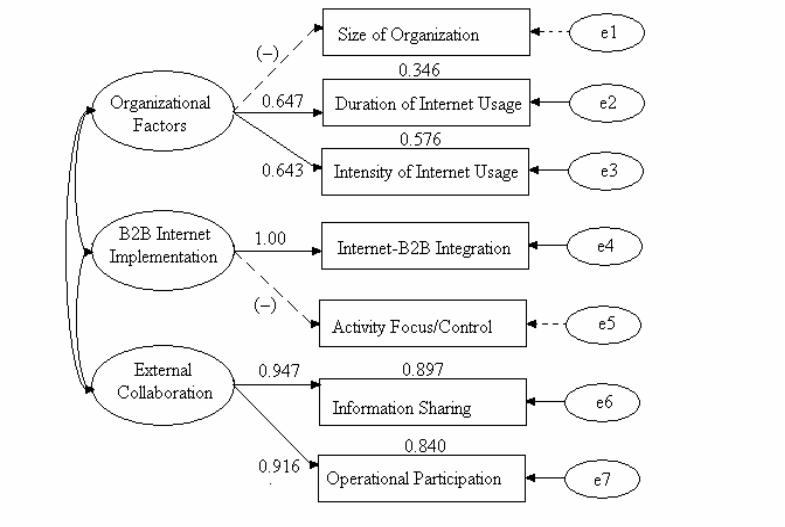
*items 5, 6 and 7 from section II of the questionnaire
** items 2, 3, and 4 from section BII of the questionnaire

The SPSS AMOS 4.0 software program was used for the confirmatory factor analysis. The initial confirmatory factor analysis for the proposed measurement model failed to provide a statistically significant result. Therefore, a model modification process was followed by eliminating inappropriate (not significant) items from the relevant constructs. The eliminated items are "system activity focus/control" from the B2B-Internet-implementation and "size of the organization" from the organizational factors construct.

The final measurement model fit statistics indicate an adequate level of fit. The value of Chi-square statistic is 22.20 at 17 degrees of freedom. It has a statistical significance level of 0.1771, which is well above the minimum level of 0.05 and is also well above the recommended levels of 0.1. The Goodness-of-fit Index (GFI) is 0.926, which is quite high. The Adjusted Goodness-of-Fit Index (AGFI) is 0.880. This result suggests that the differences of the predicted and actual matrices are non-significant, indicative of acceptable fit. The final validated measurement model is presented in Figure 2.

In Figure 2, the numbers on the arrows indicate a standardized regression weight and the numbers on the top of the boxes indicate a squared multiple correlation. For instance, in the case of the external collaboration construct, 89.7 % of the variance of information sharing and 84.0 % of the variance in operational participation are accounted for by the variance in external collaboration. The remaining 10.3 % of information sharing and 16.0 % of operational participation can not be explained by this model.

Figure 2 Confirmatory Factor Analysis of the Model



DATA ANALYSIS AND RESULTS

To assess the strength of the overall relationships among constructs, correlation analysis was employed. A correlation matrix of the constructs is presented in Table 7. The correlation matrix shows that the constructs are highly correlated. In addition, there is no evidence of multicollinearity among the constructs. The criterion of multicollinearity is generally 0.9 and greater (Hair, Anderson, Tatham, & Black,1995).

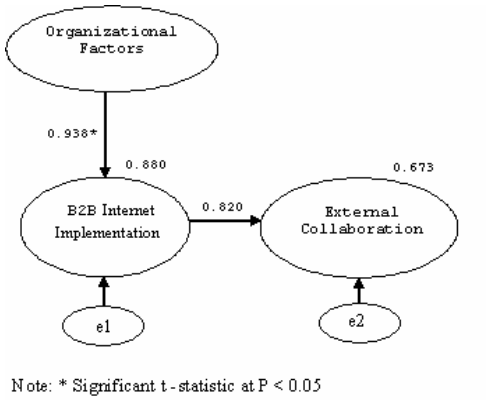
Table 7: Construct Correlation Matrix			
	1	2	3
1. Organizational Factors	-	0.757	0.651
2. B2B Internet-Implementation	0.757	-	0.792
3. External Collaboration	0.651	0.792	-
Note: Correlation coefficients are significant at the 0.01 level			

Construct correlation between organizational factors and B2B-Internet implementation is 0.757 and correlation between B2B-Internet implementation and external collaboration is 0.792, both are statistically significant at the 0.01 level. These results show that organizational factors are positively related with B2B-Internet implementation, which in turn is positively related with external collaboration: information sharing and operational participation. In other words, an organization with a longer and more intensive usage of the Internet is more likely to use Internet for B2B transactions. In addition, those with a higher level of Internet-based transactions in its supply chain would have a higher level of external collaboration with its suppliers and/or customers.

The above findings are also supported by the analysis of structural relationship as shown in Figure 3. The overall model fit measures showed an adequate level of fitness. The Chi-square value associated with the model is 36.67 at 32 degrees of freedom which yields a probability value of 0.2610. This indicates that the proposed structural relationships of the constructs and their estimated relationships are well matched with each other. The Tucker-Lewis Index (TLI) is 0.983 and the Comparative Fit Index (CFI) is 0.987. Both TLI and CFI well exceed the recommended level of 0.9, further supporting acceptance of the proposed model.

In Figure 3, the numbers on the arrows indicate standardized regression weights and the numbers on top of the circles indicate squared multiple correlation coefficients. In the case of the B2B Internet Implementation, 88.0% of the variance of external collaboration is accounted for by the variance of organizational factors. The remaining 12% can not be explained by this model. In the case of the external collaboration construct, 67.3% of the variance of external collaboration is accounted for by the variance of Internet-based transactions implementation. The remaining 32.7% can not be explained by this model.

Figure 3 Regression Results of Structural Relationships



In addition to structural equation modeling, we also use stepwise multiple regression analysis to analyze the relationship between organizational factors and Internet-B2B Integration. As mentioned in the previous section, size of the organization was dropped from the construct of organizational factors due to its low standardized regression weight. Therefore, the construct of organizational factors includes only duration of Internet usage and intensity of Internet usage. Table 8 presents the result of regression analysis regarding Internet-B2B Integration.

Table 8: Stepwise Multiple Regression for Internet-B2B Integration			
Variable	Standardized Coefficient beta	t-test	Significance
Duration of Internet Usage	0.315	4.571	0.000
Intensity of Internet Usage	0.585	8.472	0.000
$R^2 = 0.595$; Adjusted $R^2 = 0.587$; F-Ratio = 75.549; Sig. =0.000			

The result indicates the F-ratio for Internet-B2B Integration of 75.549, a strong significance level of 0.000, which suggests that organization factors have a linear relationship with the level of Internet-B2B Integration. R-square value of 0.595 indicates that 59.5% of the variance of Internet-B2B Integration is accounted for by organizational factors. Standardized coefficients beta for intensity of Internet usage and duration of Internet usage are 0.585 and 0.315, respectively. The t-test values for intensity of usage and duration of usage are 8.472 and 4.571 at significant

at the level of 0.000 and 0.001, respectively. Thus, the intensity of usage seems to explain more of the Internet-B2B integration than the duration of usage.

CONCLUSIONS

This paper investigates the impact of the Internet in the efficiency of healthcare supply chain. First, we investigate the impact of organizational factors on the level of Internet and B2B integration. The results show that, the size of the organization does not have a direct relationship with the level of such integration. This finding implies that in spite of the size of the organization, supply chain managers can and must incorporate the Internet in their day to day supply chain management transactions. In addition, other organizational factors, such as duration and intensity of internet usage, are positively related with B2B-Internet implementation. In other words, an organization with a longer and more intensive usage of Internet is more likely to use Internet for B2B transactions.

Secondly, we investigated the relationships between the Internet integration in supply chain and the level of external collaboration between trading partners. We found the while activity focus/ control is not a significant factor, those organizations with a higher level of Internet-based transactions in its supply chain would have a higher level of external collaboration with its suppliers and/or customers. This finding implies that in spite of which organization controls a given Internet based transaction, both organizations will mutually benefit from the implementation of Internet technology.

Finally, the implementation of Internet for supply chain transactions has a positive impact on external collaboration between trading partners. In other words, the users of Internet-based transactions in the healthcare industry have perceived that the implementation of the Internet in the B2B transactions has a positive effect on the collaborative supply chain activities, such as information sharing and operational participation with trading partners.

REFERENCES

Arbietman, D., Lirov, E., Lirov, R. & Lirov, Y. (2001). Internet-based transactions for healthcare supply procurement. *Journal of Healthcare Information Management*, 15(1), 61-72.

Archer, N. & Yuan, Y. (2000). Managing business-to-business relationships throughout the Internet-based transactions procurement life cycle. *Internet Research: Networking Applications and Policy*, 10(5), 385-395.

Babbies, E. (1995). *The practical of social research (Seventh Edition).* Belmont, CA: Wadsworth.

Chopra, S. & Meindl, P. (2004). *Supply chain management: Strategy, planning, and operation (Second Edition)*. Upper Sadle River, NI: Pearson Education, Inc.

Closs, D. J. & Savitskie, K. (2003). Internal and external logistics information technology integration. *The International Journal of Logistics Management,* 14(1), 63-76.

Crouch, D. (2003). Online purchasing revisited. *CMA Management*, 77(4), 37-39.

Deeter-Schmelz, D. R., Bizzari, A., Graham, R. & Howdyshell, C. (2001). Business-to-business online purchasing: Suppliers' impact on buyers' adoption and usage intent. *The Journal of Supply Chain Management*, 37(1), 4-10.

Ghosh, S. (1998). Making business sense of the Internet. *Harvard Business Review*, 76(2), 126-135.

Hair, J. F., Anderson, R. E., Tatham, R. L. & Black, W. C. (1995). *Multivariate Data Analysis (Fourth Edition).* Englewood Cliffs, NI: Prentice-Hall, Inc.

Kopczak, L. R. & Johnson, M. E. (2003). The supply-chain management effect. *MIT Sloan Management Review*, 44(3), 27-34.

Layden, J. E. (1996). Supply chain management creates new roles for IEs. *IIE Solutions*, 28(7), 36-39.

Lee, S. M. (2003). South Korea: From the land of morning calm to ICT hotbed. *Academy of Management Executive*, 17(2), 7-18.

New, S. J. (1996). A framework for analyzing supply chain improvement. *International Journal of Operations and Production Management*, 16(4), 19-34.

Porter, M. E. (2001). Strategy and the Internet. *Harvard Business Review*, 79(3), 63-78.

Poulin, E. (2003) Benchmarking the hospital logistics process. *CMA Management*, 77(1), 21-23.

Reaves, C. (1992). *Quantitative research for the behavioral sciences*. New York, NY: John Wiley and Sons, Inc.

Simatupang, T. M.& Sridharan, R. (2002). The collaborative supply chain. *The International Journal of Logistics Management*, 13(1), 15-30.

Standifer, R. & Wall, Jr. J. A. (2003). Managing conflict in B2B Internet-based transactions. *Business Horizon*, 46(2), 65-70.

Appendix A
Survey Questionnaire

I. The following questions are related to the environment of your organization.

1. Your job title: _____
2. The number of years in your organization: ____ years and ____ months
3. The number of employees in the organization: _____
4. Is your company currently using computer (information) system to manage data and inventory?
   Yes ( ) No ( )
5. Does your company currently have computer information systems for purchasing supply goods?
   Yes ( ) No ( )
6. Does your company currently have an information department? Yes ( ) No ( )
   If "Yes", how many persons work in that department? _____
7. Is your company currently using Internet or other on-line system to purchase supply goods or raw materials? Internet ( ) Other on-line systems ( ) None ( )
   a. If you answered "Internet"
      How long it has been implemented? __years and __months
      What is the portion (%) of Internet out of entire purchasing? ___
   b. If you answered "other on-line systems"
      Please specify what type of system you are using _____
   c. If you answered "none"
      Please specify your purchasing methods _____

II. The following questions are related to the operational relationship between you organization and your major suppliers. Based on your experience and perception, please circle or check on the appropriate number. (1- strongly disagree, 3- neutral, 5- strongly agree)

1. Your organization has close relationships with your major suppliers with common objectives.
2. Your organization effectively shares operational information with your major suppliers.
3. Your organization and your major suppliers participates each other for operational purposes, such as forecasting and operational plans.
4. Throughout the close interrelationship between your organization and your major suppliers, operational flexibility is increased.
5. Operational system for supply chain transaction between your organization and major suppliers is mainly controlled or focused by you, the buyer.
6. Operational system for supply chain transaction between your organization and major buyers is mainly controlled or focused by them, the buyer.
7. Your organization and your major suppliers are systematically and fully integrated in their purchasing or selling transactions.

A LONGITUDINAL INVESTIGATION OF SPAM: PRE- AND POST- CAN-SPAM LEGISLATION

Peggy Osborne, Morehead State University
Michelle B. Kunz, Morehead State University

ABSTRACT

This study examined the impact of the Can-Spam Act of 2003. A review of tactics used by "spammers" to avoid filtering software and circumvent the legal requirements was examined. Tactics in this study include the use of counterfeit characters, gibberish in the subject line, hidden agendas, invalid return addresses and misleading subject lines. A content analysis was also used to assess the most common types of messages received. The research was comprised of three studies. The first study was conducted four months prior to Can-Spam legislation. The second study was conducted four months after the Can-Spam Act became law, and the final study was conducted one year later, January 2005. Findings were significant for legitimacy of valid email sources, and between the first two studies. Final results of the third follow-up study, one year after the Can-Spam legislation went into effect shows that the law has not been effective in reducing the amount of spam, nor have avoidance tactics been significantly reduced.

INTRODUCTION

According to the Interactive Advertising Bureau (IAB) and Pricewaterhouse (PwC) advertising on the Internet reached approximately $2.43 billion by the third quarter of 2004 (Anonymous, 2004). This represents a 35.3% increase over the same quarter in 2003. Based on the $7.3 billion in revenue during the first nine months of 2004, it should be a record year. Although the industry is experiencing rapid growth in the use of online shopping, the number of spam messages is creating

some doubt as to the effectiveness of this media for the future. AOL customers are found to be more likely to click the "report as spam" button than to use the opt-out links provided in the e-mails themselves. McGann (2005) reported that Osterman Research found that because of the increase in the number of spam messages consumers receive, 44 percent report they have decreased their use of email and the Internet in the last year. With this level of decreased usage, there will be a significant impact on legitimate online marketers. Miller (2004) found that as much as 17 percent of all legitimate e-mails are being blocked by ISPs through spam filters.

Spam has penetrated the online environment at rates that may be considered equivalent to an epidemic of catastrophic proportion. Individuals and businesses alike are forced to spend a significant amount of time removing the spam from their daily routines. Erv Shames, former president of Kraft USA, criticized the online industry for tolerating the presence of "spam". He indicated that about 45% of all e-mail is made up of commercial messages unrequested and unwanted by their increasingly angry targets (Elkin, 2003). According to some reports, the increase in spam is costing companies anywhere between $10 billion and $87 billion a year. Message Labs, a London-based Internet security firm has predicted spam to account for 70 percent of all e-mail by April 2004 (Landers, 2003). Jupiter Research reported that blocking legitimate e-mail cost marketers $203 million in 2003 and will jump to $419 million by 2008 (Jakobson, 2004). Henson Rogers, VP of Information Technology for Odyssey Health Care, Inc., reported that if one half of his company's 1000 employees spent five minutes daily dealing with spam e-mail, the cost to the company would be approximately $260,000 per year (Shein, 2004). His comments are based on the fact that every junk message that an employee deals with personally cuts into productivity for the company. The spam clogs company networks and reduces company revenue by slowing legitimate operations. McGann (2004) reported that spam consumed an average 10 8-hour work days per year, and costs employers approximately $2000 per employee. The number of messages delivered to members' spam folders fell 60 percent from a year earlier. A corporate e-mail security firm, Tumbleweed Communications Corp., reported overall spam volumes to still be increasing, making up about 80 percent of the company's inbound e-mail compared to 55 percent at the end of 2003. This company reported estimates of two trillion spam messages to be on the Internet in November of 2004 and at least 25 percent more in December as a result of the holiday (Richmond, 2004). Feig reports that currently the cost of spam to non-corporate users is about $225 million and the cost to all U.S. corporations is about $8.9 billion.

Recent research (Claburn, 2005) indicates spam filtering on average eliminated 68% of spam in 2004. In November of 2004, AOL received an average 2.2 million, daily reports of spam from its subscribers, down substantially from the 11 million daily reports a year earlier. A Nucleus Ferris Research of San Francisco, estimated that spam cost US business nearly $10 billion annual in lost productivity, anti-spam technology and technical support (Costanzo, 2004).

A Wall Street Journal report (Blackman, 2003) in August 2003 reported that Radicati Group, a market-research firm, predicted the number of daily spam messages to be more than 50 billion by 2007 and costs reaching almost $200 billion a year. Consumer response to the unwanted email includes a reduction in the use of e-mail. In a study by Pew Internet & American Life Project (Greenspan, 2003), 60 percent of those responding indicated they have reduced their e-mail usage because of spam and 73 percent avoid giving out their e-mail addresses. Results also indicate that while e-mail users receive slightly more messages in their work, the proportion of spam in personal accounts is higher. This study also reports that 86% of consumers delete the e-mail immediately without opening, 67% click remove me, 33% click to get more information, 21% report the spam to their ISP, and 4% report the unwanted email to a consumer or government agency. However, at least 7% report they order a product or service, 7% provide personal information, and 1% give money as a result of the unsolicited commercial e-mail (UCE).

In a recent article, Reda (2003) reports that spammers can send up to 650,000 messages every hour from an inexpensive e-mail server. Sephos, Inc., Richmond (2004) found that often spammers use computers compromised by viruses and hijacker programs to relay spam anonymously. Sephos estimated that 30 percent of all spam is generated by infected computers. By using the hijacked computers, spammers often avoid or evade the filters used to block e-mail using "blacklists" of known spammers and make it more difficult to trace the actual spammer. This study further reported that about 400,000 infected consumer PCs are being used as spam relay points. According to Susan Reda, Executive Editor of Stores (Reda, 2003), about 50 percent of all messages individuals and businesses receive is spam and at least 66% of that spam is fraudulent by hiding text in graphics so it can't be identified as spam, sending URL's as the body of a message or hijacking company servers. Multi-channel retailers are being caught in the crossfire of consumer demand for less spam and the level of filtering provided by many ISP's. The problems for these retailers include the steady decline in the number of e-mails being delivered or opened. According to this report, AOL blocks up to 780,000,000 spam e-mails from member mailboxes every day. It is expected that $653,000,000

in sales revenue will be generated from anti-spam and content filtering solutions in 2003 and reach $2.4billion by 2007.

Prior to the 2004 Can-Spam Act, the FTC published online information for consumers on how to stop unwanted email. (www.irs.gov) (FTC, 2002). The FTC recommended consumers reduce spam by:

1. not displaying email address in public
2. checking the privacy policy when submitting an address to a web site
3. read and understand the entire form before transmitting personal information through a web site.
4. use two email addresses (one disposable)
5. use unique email address
6. use a filter

The FTC reported the most common spam scams to be chain letters, work-at-home schemes, weight loss chains, credit repair offers, advance fee loan scams, and adult entertainment (Teinowitz, 2003). In 2003 the FTC received more than 110,000 examples of spam on a daily basis and had a database of over 42 million spam messages.

The public and industry outcry for control of the unsolicited e-mail led to legislative action. On December 8, 2003 Congress sent President Bush a bill designed to curb the explosive growth of spam. This bill was called "Controlling the Assault of Non-Solicited Pornography and Marketing Act (http://www.spamlaws.com/federal/108s877.html). Many believed this bill would allow consumers to opt out of unwanted email ads, which accounted for more than half of e-mail traffic. Firms violating this law could be fined $250 per email for sending repeat messages to addresses that opt out of future ads. Companies may be fined up to $6 million.

The Can-Spam Act has five basic requirements: 1) emails may not contain false and misleading messages, 2) must have functioning return address and an opt-out mechanism that prohibits mailings after the 10-day opt-out period 3) must contain disclosure requirements (identify as advertisement, 4) provide notice of opt-out, and a warning label for sexually oriented material), and 5) prohibits aggravated violations, such as harvesting addresses (Manishin & Joyce, 2004). The requirement that consumers must contact each sender to opt-out of future email instead of forcing senders to have an opt-in permission has received criticism from

the industry. Other limitations of the law include preempting some state laws, prohibiting private citizens from suing spammers, and allowing only state attorneys general or Internet service providers to sue (Gross, 2005). This legislation is a move in the right direction, however, legislation alone will not be able to stop the spam, since spammers often operate outside the law anyway. In order to control the proliferation of spam, it will take legislation, increased technology, and legal action against the violators. On January 1, 2004 the new federal anti-spam law went into affect. These requirements were listed and discussed above. This law permits tougher penalties for use of e-mail addresses from Web sites, use of automated tools to create multiple e-mail accounts, federal agencies to seek jail time, states to seek civil penalties up to $2 million and Internet service providers up to $1 million, and a federal study to create a do-not-spam list. However, Brightmail Inc. reports that 58 percent of incoming e-mail one week after the law took effect was spam, no change from the previous month (Jesdanum, 2004).

By mid-January 2004, it became apparent that the new law would not solve the spam e-mail problems. The Credit Union Executive Society (McDonald, 2004) reported that in an analysis of over 100 opt-in messages, 44 percent did not comply with one of the simplest requirements of the new law, a postal address in the body of each message. Mangalinden reported that Time Warners' AOL, Earthlink Inc., Microsoft Corp., and Yahoo, Inc. have filed six civil lawsuits against hundreds of alleged spammers. The problem is that all but seven of the 222 defendants are unnamed. The Internet providers cannot confirm true identities of the senders of the spam. Brightmail, maker of anti-spam technology, found further evidence of the difficulty in identifying and controlling spammers. In a study conducted by their firm, Brightmail found that in February 2004, 64 percent of all e-mail traffic was spam, up from 58 percent in December. In March of 2004, 68 percent of all email was spam. This was identified through a filtering process that filtered 2.93 billion fraudulent e-mails, up 25 percent from the previous month. MXLogic had similar results and reports only 3 percent of the e-mails received had met the FTC requirement for postal addresses by mid-February, 2004 (Marson, 2004). Although action is under way to reduce the amount of spam, the volume of spam during the first month the act was in effect actually increased and has climbed since. The Radicati Group predicted the number of spam messages worldwide to be about 35 billion in 2004, this is more than double the amount in 2003 (Garretson, 2004). According to a report in InformationWeek (Anonymous, 2004), Postini Inc, a company that processes 2.4 billion messages per week for 4000 business clients, 88% of all email in November of 2004 was spam, phishing, viruses, or

directory-harvest attacks. This is further evidence that the Can-Spam Act did not stop spam, spammers are simply becoming more sophisticated and are looking for new ways around the law. Feig reports that of the 31 billion e-mail messages per day, 12.4 billion are spam. On the average, an email user will receive at least six spam messages per day.

LEGAL ISSUES

The USA Today reported that there are 1,000 to 2,000 spammers worldwide with approximately 200 accounting for up to 90 percent of about 2 trillion junk e-mail messages each year (Swartz, 2004). Although Swartz reports that many treat the anti-spam law like jaywalking, many are starting to leave the business due to the convictions others have received. Damon DeCrescenzo, one of the world's biggest spammers, dropped out of the business during 2004 as a result of the new federal anti-spam law. Fielding (2004) reported that in September 2004, approximately 4 percent of unsolicited commercial e-mail complied with the Can-Spam Act.

In November, two North Carolina residents became the first to be convicted of felony spamming charges in Virginia (Feig, 2004). In December of 2004 a federal judge in Davenport, Iowa awarded an Internet service provider more than $1 billion; AMP Dollar Savings was ordered to pay $720 million, Cash Link Systems of Miami, Florida was ordered to pay $360 million, and Florida based TEI Marketing Group was ordered to pay $140,000. Although the judgment was received, the ISP provider does not expect to receive payment.

Manishin and Joyce (2004) identified three legal issues involving the Can-Spam Act. First there is question regarding the constitutionality of the Act. This is based solely on attempts to have the do-not-call list found to be unconstitutional. Second, there is concern that the federal law preempts the state laws, many of which were much more restrictive. The third major issue is the extraterritorial jurisdiction, especially between foreign statutes such as the European Union laws which are much more protective.

The Internet Crime Complaint Center, a joint effort by the FBI and the National White Collar Crime Center, has refined its databases, shares data, and provides education and training to federal and state agencies regarding techniques used by spammers, tactics to investigate spam schemes and the tools available as a result of the Can-Spam Act (Cox & Marson, 2004). In late October and early November of 2004, Congress passed several anti-spyware measures. The I-SPY Act calls for the

FTC to oversee online software distribution and the SPYBLOCK Act regulates advertising delivered via interactive software and spyware designed to hijack end-user's computers. As of December 2004, the FTC had filed five suits under the CAN-SPAM Act. In addition Massachusetts and Washington have filed suit under the federal law and four major ISPs have gone after hundreds of spammers (Garretson, 2004).

PURPOSE OF STUDY

The overall purpose of this study was to investigate the preponderance of spam, and the tactics employed by spammers. Furthermore, the researchers wanted to examine the quantity of spam received prior to and following passage of the Can-Spam Act. Specifically the researchers were interested in determining what percentage of total email received was spam and how effectively the Can-Spam Act controlled spam.

STUDY 1

According to Teinowitz (2002) the FTC has reported that about two-thirds of all e-mail consumers receive is misleading. They describe the use of deceptive sender addresses and subject lines as those that exceed the number of characters allowed and phony offers found within the spam mailer. Currently the FTC believes 40 percent of spam e-mails contain text that appears deceptive, 44 percent use a fraudulent subject or sender address, and approximately one third have phony "from" addresses. Many of the e-mails mislead the consumer by falsely suggesting the message is from a friend or business associate. Spammers use several different techniques to avoid e-mail filters. Some of the most common methods include counterfeit characters in words, gibberish (literally letters that don't comprise words) in the subject line, hidden agendas - use of codes or written in white on white background, and treacherous tracks - incorrect email addresses (Rapoport, 2003). Additionally, the researchers wanted to determine if the "Can-Spam Act" was effective in reducing the avoidance tactics used by spammers by comparing the total number of spam messages received prior to the implementation of the act to the total number of spam messages received after the Can-Spam Act became federal law and the effectiveness one year later.

The specific research questions for the initial study were:

1. What percentage of spammers used the following avoidance tactics?
   a. Hidden agendas
   b. Gibberish in subject line or body
   c. Counterfeit characters
   d. Invalid return address
   e. Misleading subject line
2. What are the most common content "offenders?"

Methodology of Study 1

The two researchers monitored their individual email on the university server for a period of one week, during September 2003. Each email was evaluated to examine the most common tactics being used by "spammers." It should be noted that the university did not have any spam filtering software on the email server. However, information technology personnel manually block email from individual senders that are subjectively classified as serious offenders. Therefore, some messages were systematically blocked, but not technically filtered. For the purpose of this study, the tactics investigated include: agreement between the subject line and the body of message; legitimacy of an unsubscribe, opt-out provided by the sender; the use of counterfeit characters in the subject line; and gibberish in the subject line or body of the message. In addition, the researchers examined hidden agendas and whether or not the email address of the sender was a valid address.

The authors saved and printed emails identified as spam sent to their respective academic computing e-mail account for one week (7 days). A total of 326 spam messages were received, one account with approximately 113 messages, the other 211 messages. Each message was analyzed and the following data items were noted:

1. sender identification (legitimate email address?)
2. subject line of the message
3. content of the message
4. if the subject and body message content agreed
5. if there was the option to unsubscribe from a list

6. if the message contained counterfeit characters
7. gibberish in the subject line
8. hidden agenda
9. if there was a valid email or active link to unsubscribe

Results of Study 1

While it was presumed that many of the spam messages received were duplicated, in actuality this was not the case. There were several spam scams present in the dataset, as suggested by the FTC. These included: pornography, credit offers and low-rate loans, discount drugs, and money making schemes. See Table 1 for frequencies of the most prevalent content. Further analysis of the data reviewed the nine tactics listed above and usage rate for each. Results of this analysis found over 28% of the messages received did not have agreement between subject lines and body content. Over one-third contained gibberish, along with 17% that had counterfeit characters. Seventy-one percent did NOT provide an unsubscribe option, and almost 30% contained a hidden agenda, while only slightly more than one-fourth (28%) originated from a valid email address. Specific frequencies can be found in Table 2.

Since only slightly more than one-fourth of the messages were received from valid email addresses, a chi-square test of independence was calculated comparing the validity of the sender email/unsubscribe address and utilization of other tactic variables. Results were statistically significant for all tactic variables. Specific chi-square values and significance levels are presented in the Table 3, Chi-square Analysis.

Results of the cross-tab analysis found a greater number of messages with a valid email address had an unsubscribe option, slightly more exhibited subject message agreement, and fewer contained gibberish, counterfeit characters, or a hidden agenda. This would suggest that legitimate email marketers were attempting to put forth an "honest effort" in their email marketing tactics, while true "spammers" were definitely employing a high percentage of hidden agenda, gibberish, and not allowing receivers to unsubscribe.

Table 1 Most Prevalent Content Categories Fall 2003		
Spam Content	N=325	
Adult/Pornography	4	1%
Credit	5	1.5%
Discount Drugs	73	22.4%
Low rate loans	29	8.9%
Money making	19	5.8%

Table 2 Frequency of Spam Scam Tactics Fall 2003		
Variable	Freq	Percent
Subject Body do not agree	87	28.7
No Unsubscribe option	228	71.7
Use Counterfeit characters	55	17.3
Rambling/gibberish	121	37.9
Hidden Agenda	93	29.7
Invalid email	226	72.0

Table 3 Chi-square analysis Valid Email Fall 2003			
Variable	X^2	df	*p*
Unsubscribe option	306.23	1	.000
Gibberish	18.52	1	.000
Counterfeit characters	6.86	1	.009
Subject agreement	11.22	1	.001
Hidden agenda	7.79	1	.005

STUDY 2

Methodology of Study 2

During late spring of 2004, the researchers repeated the original data collection procedure for the purpose of comparison, between the pre- and post-Can-Spam Act. It seemed to each researcher that their individual email accounts contained a much larger percentage of spam, so this time each researcher counted the total number of emails received daily, and the number of these emails that constituted spam. Results, as seen in Table 4, show that three-fourths or more of the email received each day was actually spam. This finding supports the prediction of Message Labs that spam would account of 70 percent of all email by April 2004 (Landers, 2003). However, it should be noted that while the university did NOT have any spam filters in place during the study at any time, Information Technology department would block the worst offenders before email reached the ultimate receiver.

The data set was analyzed for the prevalence of body content. The most common types of content included: adult/pornography, low-rate loans, credit, discount drugs, and money-making schemes. The researchers noted a significant increase in the amount of pornographic messages. During the second series of data collection it was noted that the amount of pornography had increased almost ten-fold. Messages containing credit offers were more than slightly double those received in the fall. However the percentage of discount drug offers and money making schemes had decreased from 22.4% and 5.8% to 15.3% and 2.1%, respectively and low rate loan messages decreased slightly, 8.9% in the fall to 7.3% in the spring data collection. See Table 5 for specific frequencies and percentages.

Content analysis of the spam tactic variables for the spring 2004 showed that the number of messages exhibiting agreement between the subject and body decreased from almost three-fourths (2003) to slightly less than half, 48.6% in the spring data set. In addition, messages with a hidden agenda also decreased by almost 30%. The percentage of messages containing an unsubscribe option increased to slightly more than half, 52.6%, which was not quite twice the percentage of those present in the fall. The presence of counterfeit characters and gibberish increased, to 50.1% and 42.3% respectively. The most alarming result was the substantial decrease of messages containing an actual valid email or

unsubscribe option. This decreased from 28% in the fall of 2003, to only 12% in the spring of 2004.

Chi-square analysis and cross-tabs were again calculated comparing the validity of the sender email/unsubscribe address and utilization of other tactic variables. Results were statistically significant for all tactic variables. Specific chi-square values and significance levels are presented in the Table 6. Cross-tab analysis found that more of the messages containing a valid email address also exhibited agreement between subject line and body content, an unsubscribe option, while fewer exhibited counterfeit characters, gibberish, and a hidden agenda. These results would suggest that while fewer messages were coming from a valid email address, those individuals sending legitimate email marketing messages were now using fewer scam tactics, and it could be inferred, attempting to follow the new legislative requirements.

Table 4 Frequency of Spam Received - Spring 2004

Day	Account A			Account B		
	Total	#spam	%spam	Total	#spam	%spam
Sunday	79	69	97.34	13	11	84.62
Monday	109	89	81.65	21	18	85.71
Tuesday	94	79	84.04	19	17	89.47
Wednesday	108	72	66.67	27	23	85.18
Thursday	92	69	75.00	24	21	87.50
Friday	93	73	78.49	26	17	65.38
Saturday	65	56	86.15	25	19	76.00
TOTAL	640	507	79.21 avg.	155	126	81.29 avg.

Table 5 Most Prevalent Content Spring 2004		
Spam Content	N=626	
Adult/Pornography	62	9.9%
Credit	23	3.6%
Discount Drugs	96	15.3%
Low rate loans	46	7.3%
Money making	13	2.1%

Table 6 Frequency of Spam Scam Tactics Spring 2004		
Variable	Freq	%
Subject Body do not agree	322	51.4
No unsubscribe option	297	47.4
Counterfeit characters	314	50.1
Rambling/gibberish	265	42.3
Hidden agenda	62	9.9
No valid email	552	88.0

Table 7 Chi-square analysis Valid Email Spring 2004			
Variable	X^2	df	*p*
Unsubscribe option	46.03	1	.000
Gibberish	54.74	1	.000
Counterfeit characters	64.22	1	.000
Subject agreement	23.09	1	.000
Hidden agenda	2.183	1	.000

COMPARING STUDY ONE AND STUDY TWO

Chi-square analysis was performed to compare the data collected in the fall 2003, versus spring 2004. Results were statistically significant for five of the six spam tactics. The only variable not significant was the use of gibberish in the subject line to avoid filtering software. Specific results are presented in Table 8. Analysis using cross-tabs provided insight comparing the fall 2003 data frequencies of the variables compared to the spring 2004 occurrences of each agenda item. Although results found that the percentage of messages that provided an unsubscribe option almost doubled, the use of counterfeit characters more than doubled. The spring 2004 dataset contained fewer messages that had a hidden agenda, agreement of the subject and body, and most importantly, the number of messages sent from a valid email address decreased by more than half. These results indicate that while the Can-Spam Act has had an impact for legitimate email marketers, spammers have increased their use of scamming and avoidance tactics. It would appear that spammers have gone "underground" so that they can't be traced.

Table 8 Chi-square comparison 2003 versus 2004

Variable	X^2	df	*p*	Tau	*p*
Unsubscribe option	54.82	1	.000	.058	.000
Gibberish	2.42	1	.120	.003	.075
Counterfeit characters	100.08	1	.000	.105	.000
Subject agreement	26.61	1	.000	.028	.000
Hidden agenda	54.55	1	.000	.057	.016
Valid Email	34.05	1	.000	.036	.000

STUDY 3

The purpose of the third study was to analyze the flow of spam to the researchers' email accounts, one year following implementation of the Can-Spam Act. The research again tracked the spam received in their respective individual email accounts, and compared the amount of spam received to legitimate emails.

The university had implemented a spam filter in late fall of 2004. Therefore, during this study, the majority of spam was placed in a sub-folder on individual email accounts. Researchers could scan this folder and determine if the email was legitimate, and if so it then had to be released to the email account. However, the contents of the email body in the spam folder could not be examined unless it was released to the email account. Therefore, the researchers determined it would be advisable NOT to examine the actual body of the email for contents and agreement with the subject line, unsubscribe option, or for a valid email address. Rather, this study would examine the quantity of spam received, and the use of counterfeit characters and gibberish in the subject line, as well as the most frequent content in the subject line.

Each researcher recorded the information contained in the spam filter daily report, and checked individual email for additional spam messages that got through the filter. Results are presented in Table 9. Researcher A noted that the number of spam messages was approximately double the number received the previous spring term, while the total number of spam messages was consistent between the two studies for Researcher B.

Table 9 Frequency of Spam Receipts Spring 2005

Day	Account A			Account B		
	Total	#spam	%spam	Total	#spam	%spam
Monday	191	179	92	21	18	85.71
Tuesday	208	167	80	19	17	89.47
Wednesday	228	213	93	27	23	85.18
Thursday	226	191	85	24	21	87.50
Fri-Sun	500	463	93	26	17	65.38
TOTAL	1353	1210	89% avg.	1823	156	86% avg.

The tactics examined in this study were the use of counterfeit characters and gibberish. Use of counterfeit characters decreased substantially overall, from 50% in 2004 to 8%, but the use of gibberish increased slightly, from 42% to 49%. See Table 10 for specific frequencies in the 2005 data. However, it should be noted that Researcher A's account contained such a significantly large number of messages

containing gibberish in the subject line that it was impossible to determine the content of the messages in this account. Table 11 shows the frequency of gibberish and counterfeit characters, across the 2004 and 2005 data for the individual accounts.

Table 10 Frequency of Spam Tactics January 2005

Variable	Freq	Percent
Counterfeit characters	114	92
Rambling/gibberish	675	49

Table 11 Frequencies 2004 vs 2005 Gibberish between 2 accounts

	2004				2005			
	A		B		A		B	
	Freq	%	Freq	%	Freq	%	Freq	%
Counterfeit	297	57	17	14	65	5	49	9
Gibberish	254	50	11	9	671	55	4	0.7

Chi-square analysis and cross-tabs were calculated comparing the frequency of gibberish and counterfeit characters for years 2004 and 2005. Results were statistically significant. Specific chi-square and significance levels are presented in Table 12. Cross-tab analysis found that while messages containing gibberish were less than expected in 2004, they were greater than expected in 2005. The inverse was found for the use of counterfeit characters in the two years. The individual researchers noted what appeared to be a significant difference between the use of these two tactics in the individual accounts. It should be noted that the use of gibberish increased from 50% to 55% for researcher A, and increased from 5% to 9% for researcher B. The use of counterfeit characters significantly decreased for Research A, going from 57% of spam received in 2004 to 5% of the spam received in 2005; however counterfeit characters decreased from 14% in 2004 to 9% in 2005 for researcher B. Therefore, another chi-square analysis and cross-tabs were calculated comparing the frequency of these two tactics for Researcher A and Researcher B. Results were statistically significant. Specific chi-square and

significance levels are presented in Table 13. Cross-tab analysis found that Researcher A's account had significantly more gibberish while Researcher B's account had much less. Cross-tab analysis for the use of counterfeit characters found that Researcher A's account had fewer message than expected employing this tactic, while Researcher B's account show expected levels.

The most frequent content of spam messages included adult/pornography and discount drugs. The frequency of credit offers, discount loans and money making offers decreased to only a handful or less, see Table 14 for frequencies of content.

Table 12 Chi-square comparison 2004 versus 2005

Variable	X^2	df	*p*	Tau	*p*
Gibberish	7.18	1	.000	.004	.000
Counterfeit char.	452.03	1	.000	.225	.000

Table 13 Chi-square comparison Research A vs B for 2005

Variable	X^2	df	*p*	Tau	*p*
Gibberish	167.19	2	.000	.072	.000
Counterfeit char	379.6	2	.000	.161	.000

Table 14 Most Prevalent Content Spring 2005

Spam Content	N=1384			
	Acct A	Acct B	Total	%
Adult/Pornography	36	25	71	5
Credit	0	0	0	0
Discount drugs	90	39	129	9
Low rate loans	1	2	3	.002
Money making	0	0	0	0
International source	346	44	390	29

COMPARISON AND ANALYSIS ACROSS THREE DATA SETS

Comparing the three datasets shows the following trends:

1. The number of spam messages increased substantially with each year, more than doubling from May of 2004 to January of 2005.
2. The use of counterfeit characters increased substantially in the spring of 2004, but had significantly decreased in the spring of 2005.
3. The use of gibberish has continued to increase at approximately 5% with each year's data collection.

Specific frequencies for the number of spam, and percentage of spam containing counterfeit characters and gibberish can be found in Table 15. Chi-square analysis comparing the three data sets found the differences in use across the three years was statistically significant, and results are presented in Table 16.

Table 15 Frequency of Spam Receipts for all 3 data sets

Year	Frequency	%Counterfeit	% Gibberish
2003	326	16.9	37.1
2004	626	50.2	42.3
2005	1384	8.2	48.8

Table 16 Chi-square Comparison 2003, 2004, 2005

Variable	X^2	df	*p*	Tau	*p*
Gibberish	19.41	3	.000	.008	.000
Counterfeit char	466.05	3	.000	.119	.000

SUMMARY

The questions this study attempted to answer were: what percentage of spammers use avoidance tactics, what content was most common, and how effective

has the Can-Spam legislation been in controlling spam? Results found that prior to the Can-Spam Act, the majority of spammers used hidden agendas, did NOT provide an unsubscribe option and came from an invalid email address. Post-Can-Spam Act data show that more of the messages received provided an unsubscribe option, now slightly more than half; half contained counterfeit characters, and slightly less than half contained gibberish. Most startling was that fact that the percentage of messages coming from a valid email address decreased from 28% in the fall to only 12% in spring 2004. However, validity of email address could not be verified in the third study. Furthermore, the number of spam messages received had almost doubled. The answer to the question posed at the outset of this study is: Has the Can-Spam Act been effective in controlling spam? These results clearly show "spammers" are avoiding the requirements set forth in the legislation.

Both the private sector and business organizations continue to call for control of the spam email crisis. It has been predicted by some that email will no longer be recognized or utilized as a major communication tool unless the spam epidemic can be controlled. Some individuals suggest charging for email, the development of "no email" lists, additional government legislation and involvement, prosecution of violators, and an outright closure of the email process. In an effort to respond to these and other issues in dealing with the problems created by spam, TRUSTe, a leading provider of privacy certification and seal programs, testified before a Senate hearing that more than half of consumer complaints are a result of unwanted spam. As a result of these complaints, ISP's are creating filters, which block about 40% of all e-mail as spam. This sometimes creates a "false positive" resulting in about 15% of legitimate e-mail not getting delivered (Hodge & Mattox, 2003). In an effort to provide consumers with a method to screen unwanted email and still receive legitimate messages, IronPort Systems and TRUSTe launched the Bonded Sender Program. This Program allows legitimate senders of mail to avoid being blocked by overly aggressive spam filters by allowing senders to identify themselves, adhering to standards and posting a financial bond (Landis, Matick, Hodge, & Sullivan, 2003). In October 2003, the IAB (Interactive Advertising Bureau) with TRUSTe released the "Email Marketing Pledge" - a set of email marketing guidelines (IAB, 2003). These guidelines require informed consent before sending email. The Pledge is expected to increase industry accountability by more clearly differentiating between legitimate mail and spam.

Until consumers can easily differentiate between spam and legitimate email, they will employ tactics to make their inbox manageable. In many instances these

actions mean the marketing messages sent, even those sent by legitimate senders will not reach the receiver. Consumers reported that during the Holiday 2004 shopping season, they simply deleted additional email they received (McGann, 2005). Furthermore, 27% unsubscribed from email lists that sent them messages too frequently; 23% regularly used the ISP's mail program "this is spam" button. These numbers, and the increasing number of spam filters being employed by individual consumers, as well as ISP's and corporate mail servers, should serve notice to legitimate email marketers. Marketers should move from mass marketing to targeted marketing, as well as be sure that the receiving consumer is a legitimate customer who wishes to receive email marketing messages.

It appears that the Can-Spam law, in effect for a year, has not been successful in squelching unsolicited e-mail (Hulme, 2005). Even worse, it is estimated that about 75% of email is spam (Snyder, 2004); the volume of spam is so high, that it has dominated Internet message flow. Christopher Conkey (2005) fears the legislation will not make much of a dent in the steady flow of illegal spam, since industry analysts report the phenomenon worsened in 2004, and most estimates indicate spam account for 70-80% of total email traffic. Results of this study support these findings. The Can-Spam Law has had little if any effect on the number or type of spam emails being generated. There is clear evidence that "spammers" are becoming savvier in the types of avoidance tactics utilized. Companies must develop means to filter and control the amount of spam email messages received before the public becomes so distrustful that they will no longer open any commercial email message. The results of this study should be a great concern to legitimate email marketers, as the current state of the email marketing environment shows that spam is a serious two-fold threat: first to email marketers ability to get their messages through the clutter of spam, and to consumers' ability to trust the message senders.

REFERENCES

Anonymous. (2004, November 15). 2004 interactive advertising revenues total over $2.4 billion: Fourth record-setting quarter. Retrieved January 20, 2005, from http://www.iab.com/news/pr_2004_11_15.asp

Anonymous. (2004, December 6). Ok, spam, enough already. *InformationWeek*, 12.

Blackman, A. (2003). An 'easy target' for e-mail spam. *The Wall Street Journal*.

Claburn, T. (2005, January 17). Spam: Are we winning the fight? *Information Week*, 20-21.

Conkey, C. (2005, January 12). Ftc wins order to shut down spam from adult web sites. *Wall Street Journal*, 2.

Costanzo, C. (2004, December 1). You've got spam! *Community Banker*, 13, 24-28.

Cox, J., & Marson, C. (2004, November 20). Is the law's arm long enough? *Network World*, 21, 50-51.

Elkin, T. (2003, May 7). What online media sellers aren't doing well. Retrieved January 15, 2004, from http://www.adage.com/news.cms.?newsId=37781

Feig, N. (2004, December). Spam it! *Community Banker*, 13, 68.

Fielding, M. (2004, December 15). Can spam compliance spotty. *Marketing News*, 38, 20-21.

FTC. (2002). You've got spam:Federal Trade Commission.

Garretson, C. (2004, December 13). Federal anti-spam law gets mixed results. *Network World*, 21, 9.

Greenspan, R. (2003, October 23). Spam: Always annoying, often offensive. Retrieved January 30, 2004, from http://cyberatlas.internet.com/big…ions/ print/0,1301_3097351,00.html

Gross, G. (2005). U.S. Can spam act struggles to make a difference. *Networld World*, 27, 16.

Hodge, C., & Mattox, K. (2003, May 21). TRUSTe weighs in at senate hearing on spam. Retrieved December 1, 2003, from www.truste.org/about/ Senate_Testimony_Alert.html

Hulme, G. V. (2005). Another fight to wage: Companies buried by spam focus their attention--and resources--on the battle against spyware and adward. Information Week, 60-63.

IAB. (2003, October 13). A new front in the war on spam. IAB Informer October 13. Retrieved December 1, 2003, from http://www.iab.ent/informer/ informer_10_03.asp

Jakobson, L. (2004). First spam, now spim. *Incentive*, 178(4), 14.

Jesdanum, A. (2004, January 31). Spam is winning the war despite new laws and technology, inboxes still flooded. *Lexington Herald Leader*.

Landers, J. (2003, December 9). Skeptics wonder if anti-spam bill sent to bush will really work. *Lexington Herald Leader*.

Landis, L., Matick, S., Hodge, C., & Sullivan, M. (2003, October 13). Ironport systemstm launches next generation of bonded sender programtm program. Retrieved December 15, 2003, from http://www.truste.org/about/BondedSenderLaunch.htm

Manishin, G. B., & Joyce, S. A. (2004). Current spam law & policy: An overview and update. *Computer and Internet Lawyer*, 21(9), 1-7.

Marson, C. (2004). Ietf to lead anti-spam crusade. *Network World*, 21(15), 1-2.

McDonald, L. (2004). E-marketing can(t) spam. *Credit Union Management*, 27, 58-59.

McGann, R. (2005, January 26). Holiday e-mail campaigns receive mixed report. Retrieved February 5, 2005, from http://www.clickz.com/stats/sectors/email/ article.php/3464351

Rapoport, R. (2003, August 19). Spam senders change tactics. *Lexington Herald Leader*, C1-C2.

Reda, S. (2003). You've got spam. *Stores*(September), 26-30.

Richmond, R. (2004, December 28). AOL notes decline in junk e-mail, as trend reverses. *Wall Street Journal*.

Shein, E. (2004). Get rich quick fighting spam. CFO.com, 1.

Snyder, J. (2004, December 20). Top spam fighters offer feature diversity. *Network World*, 21, 34-38.

Swartz, J. (2004, May 6). New software laws push some spammers to log out. *USA Today*, B.01.

Teinowitz, I. (2002, September 4). Consumer groups seek tougher spam crackdown. Retrieved December 20, 2003, from www.adage.com/news.cms?newsId=35958

Teinowitz, I. (2003, April 29). Ftc attacks spam as threat to e-mail. Retrieved December 1, 2003, from www.adage.com/news.cms?newId=37726

End of ARTICLES for Volume 3, Number 1

ARTICLES for Volume 3, Number 2

ARTICLES for Volume 3, Number 2

.EDU DILEMA: THE WEB ACCESSIBILITY CHALLENGE FACING PUBLIC AND PRIVATE UNIVERSITIES

Danial L. Clapper, Western Carolina University
Debra D. Burke, Western Carolina University

ABSTRACT

In the early days of the World Wide Web a popular metaphor used to capture the essence of the web was the frontier days of the American "Wild, Wild West." It was a wide-open, self-policing, unregulated frontier and newcomers had best beware! As the Web has become an increasingly accepted part of our world, the frontier metaphor use has noticeably declined. But the de-centralized technology architecture, which was behind this metaphor, is still as true today as it was in the early days of the web. And perhaps nowhere has that decentralized model been as enthusiastically embraced as in the university setting.

From the small team of professional developers working in the admissions office to create online applications, to the part-time student workers creating departmental web pages, to the full-time and adjunct faculty putting an increasing amount of course related material and content up on the web, widely disparate groups and individuals have created a phenomenal number of web pages, often without any awareness of other groups on campus, minimal to no oversight by university technology administration or legal counsel, and frequently with little or no awareness of legal/ethical concerns such as the need to make their web pages available to people with disabilities.

This paper will propose that, although the web has become a fundamental, vital tool for universities, some of the fundamental aspects of the web -- combined with the history of how the web has been adopted on campuses -- results in a particularly daunting barrier to verifying and guaranteeing that all web pages used at the university are in compliance with the law and accessible to populations with disabilities.

INTRODUCTION

The Americans with Disabilities Act ("ADA") of 1990 was Congress' effort to eliminate discrimination against individuals with disabilities. The intent of the legislation was to insure that people with disabilities could be active and productive members of society, undeterred by artificial barriers. At the time the ADA was enacted, the World Wide Web was in its infancy and no one – including its creators – could have foreseen how in a short fifteen years the web would move from being a tool for physicists to shared research results, to being an important part of our society. In the early days of the World Wide Web a popular metaphor used to capture its essence was the frontier days of the American "Wild, Wild West." It was a wide-open, self-policing, unregulated frontier and newcomer's best beware! As the Web has grown, the frontier metaphor use has noticeably declined. Instead, the Web has become an accepted, important part of our day-to-day routine and increasingly provides the information and services that we need in our normal lives. A recent report on web usage suggests that the web has become "the 'new normal' in the American way of life; those who don't go online constitute an ever-shrinking minority" (Rainie & Horrigan, 2005). As this change occurs, as more and more information is available on the Web, it becomes increasingly important to insure that all potential users can access this information.

This seems a particularly crucial issue for universities where – not surprisingly – the web has been enormously successful. The de-centralized technology architecture, which was behind the "Wild, Wild West" metaphor, is still as true today as it was in the early days of the web. And perhaps nowhere has that decentralized model been as enthusiastically embraced as in the university setting. From the small team of professional developers working in the admissions office to create online applications, to the part-time student workers creating departmental web pages, to the full-time and adjunct faculty putting an increasing amount of course related material and content up on the web, widely disparate groups and individuals have created a phenomenal number of web pages – often without any awareness of other groups on campus, minimal to no oversight by university technology administration or legal counsel, and frequently with little or no awareness of legal/ethical concerns such as the need to make their web pages available to people with disabilities.

This paper will first provide a legal survey of relevant legislation to answer the question of legal responsibilities of public and private universities to provide accessible web pages. It will then look at the types of disability impairments that

provide barriers to using the web and explore the question of what accessibility means, and how to create web pages that are accessible to these different populations. Next it will explore why universities face some particularly daunting barriers to verifying and guaranteeing that all web pages used at the university are accessible to populations with disabilities. Finally, the paper will summarize the implications for technology managers and planners, who are responsible for university web pages.

OVERVIEW OF THE LEGAL ENVIRONMENT

Concluding that discrimination persisted against individuals with disabilities, which adversely affected both disabled Americans and society as a whole, Congress passed the Americans with Disabilities Act ("ADA") in July of 1990 in an effort to eliminate such discrimination, and to provide consistent, enforceable federal standards for addressing such discrimination. (Wehman, 1993). Congress concluded that "individuals with disabilities are a discrete and insular minority who have been faced with restrictions and limitations, subjected to a history of purposeful unequal treatment, and relegated to a position of political powerlessness in our society, based on characteristics that are beyond the control of such individuals and resulting from stereotypic assumptions not truly indicative of the individual ability of such individuals to participate in, and contribute to, society." (42 U. S. C. §12101(a)(7) (2004)). The five titles of the legislation address these problems in Employment (Title I), Public Entities (Title II), Public Accommodations (Title III), and Telecommunications (Title IV). Title V contains miscellaneous provisions relating the ADA to other laws and its implementation. The ADA extended the coverage provided by the Rehabilitation Act of 1973, which protects handicapped individuals from employment discrimination by the federal government and by private employers who either contract with the federal government or administer programs receiving federal assistance, to private entities in an expanded scope of activities. (Burgdorf, 1991).

Title I of the ADA requires employers to make reasonable accommodations for qualified employees with disabilities, so long as the accommodation would not result in an undue hardship, that is, one which entails significant difficulty or expense. (Karlan & Rutherglen, 1996). The ADA and federal regulations define the term "qualified individual with a disability" as "an individual with a disability who, with or without reasonable accommodation, can perform the essential functions of the employment position that such individual holds or desires." (42 U.S.C. §

12111(8) (2000)). In other words, a qualified individual must be able satisfy the requirements of the job, such as proper training, skills, education or experience, in addition to possessing the ability to perform the essential functions of that job either with or without reasonable accommodation.

The Act further defines disability for all Titles as "a physical or mental impairment that substantially limits one or more major life activities, a record of such of such impairment, or being regarded as having such impairment." (42 U.S.C. § 12102(2) (2000)). In contrast to cases of an individual having an actual disability or a history of an actual disability, in "regarded as" cases of discrimination a covered entity entertains misperceptions about the individual, believing either that one has a substantially limiting impairment of a major life activity, which one does not have, or that one has a substantially limiting impairment, when, in fact, the impairment is not so limiting. (Simmons, 2000; Mayerson, 1997). These "major life activities" as defined by federal regulations include functions such as caring for oneself, performing manual tasks, walking, seeing, hearing, speaking, breathing, learning, and working, in the sense that one's ability to work is significantly restricted with respect to the performance of either a class of jobs, or a broad range of jobs in various classes, as compared to the average person having comparable abilities. (29 C.F.R. § 1630.2 (2000)). The Supreme Court also interpreted the Act as including reproduction as a major life activity as well. (Bragdon v. Abbott, 1998). The term "substantially limits" is used in comparison to the average person in the general population with consideration being given to the nature and severity of the impairment, its duration, and its permanent or long-term impact. (Zappa, 1991).

Title II provides that "no qualified individual with a disability shall, by reason of such disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of a *public* entity, or be subjected to discrimination by any such entity." (42 U.S.C §12132 (2004)). The term "qualified individual with a disability" is defined as "an individual with a disability who, with or without reasonable modifications to rules, policies, or practices, the removal of architectural, communication, or transportation barriers, or the provision of auxiliary aids and services, meets the essential eligibility requirements for the receipt of services or the participation in programs or activities provided by a public entity." (42 U.S.C §12132(1) (2004)).

Title III provides, as a general rule, that "[n]o individual shall be discriminated against on the basis of a disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation…" (42 U.S.C. § 12182(a) (2004)). Illegal

discrimination includes 1) denying disabled individuals the opportunity to participate in or benefit from the goods, services, facilities, privileges, advantages, or accommodations of an entity; 2) affording disabled individuals the opportunity to participate in or benefit from a good, service, facility, privilege, advantage, or accommodation that is not equal to that afforded to other individuals; 3) providing a good, service, facility, privilege, advantage, or accommodation that is different or separate from that provided to other individuals, unless such action is necessary to provide a good, service, facility, privilege, advantage, or accommodation, or other opportunity that is as effective as that provided to others. (42 U.S.C §12182(b)(1)(A) (2004)). As a caveat, Title III requires an entity operating "public accommodations" to make "reasonable modifications" in its policies "when ... necessary to afford such ... accommodations to individuals with disabilities, unless the entity can demonstrate that making such modifications would fundamentally alter the nature of such ... accommodations." (42 U.S.C §12182(b)(2)(A)(ii) (2004)).

The phrase "public accommodation" is defined in terms of twelve extensive categories, which include, for example, places of lodging, establishments serving food or drink, places of exhibition or entertainment, places of public gathering, sales or rental establishments, service establishments, stations used for public transportation, places of public display, places of exercise or recreation, places of education, and social service centers. (42 U.S.C. § 12181(7) (2004)). Legislative history indicates that the definition of private entities, which affect commerce, and are considered places of public accommodation under Title III, should be construed liberally to afford people with disabilities equal access to the wide variety of establishments available to the nondisabled. For example, the Supreme Court held that golf tours and their qualifying rounds fit within Title III's coverage, and that a participant was within its protection. (Martin v. PGA Tour, Inc. 2001).

Although some observers argue that subsequent to its passage, courts have interpreted the provisions of the ADA too narrowly and frustrated its declared purpose (Sutter, 2000; Locke, 1997), the remedial statute may still be broad enough to embrace cyberspace. Under the law of other countries, the issue of web-accessibility for the disabled has surfaced. An individual won damages in Australia against the *Sydney Organizing Committee for the Olympic Games* for its failure to maintain a website, which was accessible to the visually impaired. (Clark, 2002). The issue is also being considered in the United Kingdom under its Disability Discrimination Act of 1995. (Sloan, 2001). It is estimated that as many as ninety-eight percent of websites are not accessible to individuals with disabilities. (Rich, et al., 2002). Is this situation problematic under the U. S. law? The answer at this

stage would have to be "maybe," and dependent in part upon whether the site is maintained by a public or private entity, or by a recipient of federal funds.

PUBLIC ENTITIES AND WEB ACCESSIBILITY UNDER TITLE II

Congressional regulation of state governments and their affiliates, like state universities, is subject to constitutional restraints, in particular the Eleventh Amendment which declares that, "[T]he Judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by Citizens of another State, or by Citizens or Subjects of any Foreign State." Congress, however, has the power under the Fourteenth Amendment to abrogate state sovereign immunity in some situations, and to create civil causes of action in order for private citizens to bring suit against state entities. For example, states can be sued under Title VII of the Civil Rights Act of 1964. Section 5 of the Fourteenth Amendment, which allows this inroad into state sovereign immunity, states in relevant part that "[N]o State shall…deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

A rich history of constitutional interpretation has defined this prohibition as being primarily applied to remedial situations involving fundamental rights or legislative classifications which are "suspect," such as the laws requiring segregation based upon race. In other words, for its legislation to be constitutional in these situations, Congress must be attempting to remedy a past pattern of discrimination by the states, such as slavery in the South. Further, it is easier for Congress to succeed in abrogating sovereign immunity if the legislation involves a fundamental right. (Nevada Dept. of Human Resources v. Hibbs, 2003). State action, which abridges fundamental rights, for example, the right to freedom of speech or religion, or the right to vote, is subject to strict judicial scrutiny; that is, it "may be upheld only if it is narrowly tailored to further a compelling interest." (United States v. Playboy Entertainment Group, Inc., 813, 2000). In contrast, legislation not involving such rights (or suspect classifications) is upheld if it bears a *rational relationship* to a legitimate state interest.

Presumably under Title I of the ADA, if state employees were required to utilize websites while performing job responsibilities, then web-accessibility could be viewed as potentially being a reasonable accommodation, depending upon the circumstances. Nevertheless, as a result of a recent Supreme Court decision, state employers in fact may have limited exposure to liability under Title I. (Rich, et al.,

2002). In 2001 the Supreme Court held that state sovereign immunity under the Eleventh Amendment bars suits in federal court by state employees to recover money damages by reason of the state's failure to comply with Title I (employment) of the ADA. (Board of Trustees of the University of Alabama v. Garrett, 2001). Although Congress would have the authority to subject state governments to private lawsuits under Title I of the ADA for the violation of Fourteenth Amendment rights (such as due process and equal protection), that result is only permissible if there has been a pattern of discrimination in hiring decisions, in this case involving persons with disabilities, which Alabama had not exhibited.

Further, the Constitution only requires that states do not irrationally discriminate against disabled persons; however, Title I of the ADA demanded more, that is, that states take steps to provide a reasonable accommodation for qualified disabled individuals. The Court observed "that States are not required by the Fourteenth Amendment to make special accommodations for the disabled, so long as their actions towards such individuals are rational. They could quite hard headedly--and perhaps hardheartedly--hold to job-qualification requirements which do not make allowance for the disabled." (Board of Trustees of the University of Alabama v. Garrett, 2001). While this in tandem interpretation of the Eleventh and Fourteenth Amendments limits the availability of damages for suits brought against state governments by the disabled under Title II, injunctive relief may still be available. (Horvath, 2004).

The Court in *Garrett* also left open the question as to whether or not the Eleventh Amendment permits suits for money damages under Title II. In a subsequent case, the Court held that, at least as far as Title II of the ADA applies to cases implicating the fundamental right of access to state courts and the administration of justice, Title II of the ADA constitutes a valid exercise of Congress' authority under Section 5 of the Fourteenth Amendment, in order to enforce that Amendment's substantive guarantees. (Tennessee v. Lane, 2004). While the right of parents to direct the education of their children may be considered a fundamental one (Wisconsin v. Yoder, 1972), the right of access to education itself has not been so defined. Therefore, applying the mandates of Title II to public educational institutions, and derivatively their websites, indeed may be an unconstitutional exercise of Congressional power, because the right implicated is not a fundamental one, and the class of persons presumably discriminated against, that is, the disabled, are not (under Fourteenth Amendment jurisprudence) members of a suspect class, who historically have been discriminated against (as are racial minorities). It may take years to resolve conclusively which areas of Title II are

enforceable, although arguably that resolution will hinge in part on the nature of the underlying right, as well as the existence of a history of civil rights violations by state actors (Eyer, 2005).

ACCOMMODATIONS IN VIRTUAL PUBLIC PLACES UNDER TITLE III

Congress may have more latitude under the Interstate Commerce Clause of the Constitution to regulate private entities under ADA. Under Title I (Employment) if qualified employees in private educational institutions are required, as part of their job, to use web pages, then employers may owe a legal obligation to make them accessible to the disabled, providing such a requirement is considered to be a reasonable accommodation, and not one that would result in an undue burden. Alternatively, it might be sufficient to make the necessary information accessible in another format.

As noted previously, Title III of the statute prohibits discrimination in privately owned and operated places of public accommodation, such as private educational institutions. The critical inquiry then, is whether or not websites should be considered places of public accommodation. Clearly Congress did not intend to embrace virtual environments when the ADA was passed in 1990, as the passage of the Act preceded the establishment of the Internet as a mainstream form of communication and of access to goods and services. Nevertheless, the Department of Justice issued an advisory letter in 1996 suggesting that the ADA covers entities on the Internet whose services are deemed to be public accommodations. (Ranen, 2002). While the issue is as yet unsettled, several commentators have argued that websites should be considered places of public accommodation (Kiedrokski, 2001; Lynch, 2004), or considered as such at least in those cases where the website has a connection, or *nexus*, to a physical place of public accommodation. (Moberly, 2004). Under this approach barnesandnoble.com would be covered under the ADA, but Amazon.com would not be covered, because Barnes & Noble has a physical presence in contrast to Amazon, which has only a virtual existence.

Some federal courts appear to be open to this type of argument in other contexts. In *Rendon v. Valley Crest Products, Ltd* (2002) hearing-impaired and mobility-impaired individuals alleged that Valleycrest Productions Limited and ABC violated the ADA by operating a telephone selection process that screened out disabled individuals, who wished to be contestants on the show "Who Wants To Be A Millionaire." The district court dismissed the complaint, but the Eleventh Circuit

reversed, concluding that the fast finger telephone selection process was a discriminatory screening mechanism, which deprived plaintiffs the opportunity to compete for the privilege of being a contestant on the *Millionaire* program. The court reasoned that the alternative approach, screening contestants the same way at the actual studio, which is clearly a "place of public accommodation," could violate the ADA; therefore, an off-site approach should be treated similarly. (Grady & Ohlin, 2004).

This issue has been addressed in a somewhat different context by several courts with respect to insurance providers, and the issue of whether insurance providers should be considered a "service establishment" under the ADA if they do not serve walk-in customers. The First Circuit concluded that the ADA applied to physical establishments whether or not they served walk-in customers (Carparts Dist. Ctr., Inc. v. Automotive Wholesaler's Assoc. New England, 1994). Likewise, the Second Circuit concluded that practices of insurers could be covered by Title III of the ADA, reasoning that the statutory term was not limited to situations involving physical access. (Pallozzi v. Allstate Life Ins. Co., 1999). The Seventh Circuit went further and suggested in dicta that the critical inquiry is whether or not the entity provides goods and services, which are open to the public. (Doe v. Mutual of Omaha Ins. Co., 1999). In contrast, the Sixth Circuit concluded that there must be a nexus between the discriminatory transaction and the physical place of public accommodation. (Parker v. Metropolitan Life Insurance Co., 1997). The Third Circuit embraced this nexus requirement as well. (Ford v. Schering-Plough Corp., 1998).

Some observers criticize the nexus approach, since it produces incongruous results, which are conditioned upon the rather artificial distinction of either being able to serve walk-in customers, or not offering such services through a physical presence. While some critics of this approach would conclude that all websites, which serve as a conduit to the provision of goods and services, are covered by the ADA (Petruzzelli, 2001; Ranen, 2002; King, 2003), others argue that the ADA does not support such an extension, and that Congress should enact alternative legislation to assure web accessibility. (Maroney, 2000; Konkright, 2001).

In 1999 the National Federation for the Blind brought a class action lawsuit against American Online under Title III alleging that the Internet provider violated the ADA because its services were inaccessible to the blind, since they were incompatible with screen access software programs for the blind. (Ranen, 2002). The issue was never resolved as the complaint was dismissed by mutual agreement between the parties, whereby AOL agreed to take steps to improve accessibility.

(Waddell, 2000). Only one case to date has considered the issue directly. In *Access Now, Inc. v. Southwest Airlines, Co*. (2002) a federal district court concluded that Southwest.com was not a place of public accommodation under Title III of the ADA, determining that the unambiguous language of the statute does not include Internet websites among the definitions of "places of public accommodation." The court reasoned that the ADA applied only to physical, concrete structures, and "[T]o expand the ADA to cover 'virtual' spaces would be to create new rights without well-defined standards." (Access Now, Inc. v. Southwest Airlines, Co., 1318 (2002)).

Plaintiffs appealed the dismissal of the complaint to the Eleventh Circuit, which declined to consider the case on its merits because the issues raised on appeal were not adequately presented in the district court. While the district court's ruling was limited to the question of whether or not a website was a place of public accommodation, on appeal the plaintiffs argued for the first time that Southwest Airlines was a place of public accommodation because it operates a "travel service" under Title III, and hence violated that Title because of the website's connection to the airline's travel services. Because the new argument depended on facts and theories not presented to the district court, involving the allegation that the violation was a result of the nexus between the inaccessible website and the travel service provided by the airline, the court declined to consider the merits of either the theory presented to the district court or the one presented for the first time on appeal.

What does this mean for private educational institutions? Included among the private entities considered to be public accommodations under the ADA are "a nursery, elementary, secondary, undergraduate, or postgraduate private school, or other place of education." (42 U.S.C. § 12181(7)(j) (2004)). But are their websites included? It would seem that in the circuits in which courts use the nexus approach, their websites would have to be made accessible, providing the institution had a "brick and mortar" physical presence. In other jurisdictions, courts might limit the application of the ADA mandate to the physical structures of the institution only.

However, the provision of education arguably dictates that another factor be considered. Title III of the ADA also provides that "[A]ny person that offers examinations or courses related to applications, licensing, certification, or credentialing for secondary or postsecondary education, professional, or trade purposes shall offer such examinations or courses in a place and *manner* accessible to persons with disabilities or offer alternative accessible arrangements for such individuals. (42 U.S.C. § 12189 (2004)). Therefore, it could be argued that the statute requires a heightened standard of accessibility for educational providers.

(Robertson, 2001). While that result does not necessarily command that the websites be made accessible, only that the information be provided in a manner that is accessible, as a practical matter, it would likely be efficient to meet the directive by providing accessible websites. At any rate, if courts do not interpret Title III of the ADA, as currently written, to include websites in cyberspace as constituting places of public accommodation, Congress still would have the power under the Commerce Clause to legislate such a result by prohibiting private websites from discriminating against disabled users. (Lynch, 2004).

THE REHABILITATION ACT

Congress amended the Rehabilitation Act of 1973 with the passage of the Work Force Investment Act of 1998, so as to require federal agencies to make their websites accessible to persons with disabilities. Section 508 of that law now provides that "[W]hen developing, procuring, maintaining, or using electronic and information technology, each Federal department or agency…shall ensure, unless an undue burden would be imposed…that the electronic and information technology allows, regardless of the type of medium of the technology (i) individuals with disabilities who are Federal employees to have access to and use of information and data that is comparable to the access to and use of the information and data by Federal employees who are not individuals with disabilities; and (ii) individuals with disabilities who are members of the public seeking information or services from a Federal department or agency to have access to and use of information and data that is comparable to the access to and use of the information and data by such members of the public who are not individuals with disabilities." (42 U.S.C. § 794d (a)(1)(A) (2002)). The law directed the Architectural and Transportation Barriers Compliance Board (*Access Board*) to develop standards governing the implementation of this mandate, which are now set forth in the Federal Code of Regulations. (36 C.F.R. § 1194.22 (2004)). While the Act does not apply specifically to states or private entities (McLawhorn, 2001), it does apply to states that receive funds under the Assistive Technology Act 1998 (29 U.S.C. § 3011 (2004)), which requires recipients to give written assurances of compliance with Section 508 of the Rehabilitation Act in order to receive grants designed to maintain permanent, comprehensive statewide programs of technology-related assistance for individuals with disabilities. All fifty states receive such grants, thereby necessitating an assurance of compliance with the federal standards. (Robertson, 2001). However, there is a sunset provision in the

Assistive Technology Act of 1998, which could terminate funding, and the corresponding need for assurances of compliance. (Myers, 2004).

Even so, Section 504 of Rehabilitation Act also provides that "[N]o otherwise qualified individual with a disability in the United States…shall, solely by reason of her or his disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination under any *program or activity* receiving Federal financial assistance or under any program or activity conducted by any Executive agency or by the United States Postal Service." (29 U.S.C. § 794(a) (2002)). The phrase "program or activity" is defined as including a college, university, or other postsecondary institution, a public system of higher education, a local educational agency, a system of vocational education, or other school system. (29 U.S.C. § 794(b)(2)(A)&(B (2002)). The Civil Rights Restoration Act of 1988 clarified a broad definition for that term, such that if a state agency or entity receives federal funding for any purpose, it is subject to liability for discriminatory practices in all its programs. (Eyer, 2005). It would seem that this section could put covered institutions at risk, if the manner in which they offered their online services to their constituents were not equally available, either through web accessibility or by some other format, to the disabled.

Moreover, a strong argument can be made that despite differences between the ADA and Section 504, the statutes are co-extensive, and claims comparable to those, which previously were brought under Title II, should be viable under Section 508, particularly since the vast majority of state entities, which are potentially immune from ADA litigation, are still recipients of federal funds. (Eyer, 2005). Nevertheless, while some courts have held that Congress constitutionally may require a waiver of sovereign immunity as a condition of receiving federal funding, or that a waiver of immunity occurs when states accept such funding, others have held that the abrogation analysis should be the same for Title II of the ADA as for Section 504 of the Rehabilitation Act, which would preclude claims by private citizens to enforce rights provided for under Section 5. (Roy, 2004). Even so, the federal government might be able to sue in their behalf, and such an action arguably would not be subject to the Eleventh Amendment, which only expressly prohibits suits "by Citizens of another State, or by Citizens or Subjects of any Foreign State."

STATE LAWS AND STATE GOVERNMENTAL ENTITIES

Independent of federal law and federal financing concerns, an overwhelming majority of states require their governmental agencies, which could include publicly

funded universities, to make their websites accessible and develop guidelines to that end. (Sweeney, 2000). Almost all states have developed web-accessibility policies or standards. (Poynter, 2003). For example, Texas state law requires all state agencies to maintain websites, which conform to generally acceptable standards for persons with disabilities. (Robertson, 2001). Twelve states have accessible information technology laws, some of which require compliance with Section 508 (e.g., California) or have established their own standards. (Myers, 2004). Moreover, states could decide to waive their sovereign immunity, like Illinois, in order to allow claims brought under civil rights legislation, such as the ADA. (Roy, 2004).

Yet, even assuming that there is a legal obligation to make websites accessible to the disabled, some might argue that there are no clear parameters to establish compliance. (Quinn, 1999). Moreover, if federal standards are applicable to state agencies under the Workforce Investment Act, they nevertheless have been slow to comply (Hammond, 2003). These problems, as well as other issues, plague the directive, assuming that there is one for private institutions under the ADA, or for states or state institutions seeking federal funds, or as required by state law.

Clearly accessibility regulations, which might pertain to university web pages, are a complicated mix of federal and state laws. The ADA, the statute which seems most relevant to the question of accessibility in web pages, was passed before the web was a significant part of our society; therefore web accessibility was not explicitly addressed by the legislation. While some federal courts seem inclined to interpret the ADA to cover websites maintained by private places of public accommodation, other jurisdictions do not. As amended, the Rehabilitation Act does explicitly cover websites, but its focus is on federal government websites. While the provision of Section 508 that extends to entities that receive funds from the federal government would certainly include most public universities, again there is no conclusive ruling that requiring public universities, which accept such funds, to have accessible web pages would not violate sovereign immunity, as might the application of the ADA itself to public universities. Most states have laws requiring accessible web pages for state government websites, which should include public universities. However, the precise requirements and penalties for non-compliance vary from state to state, and whether or not they extend to private universities would be dependent upon the particular statute.

While the legal environment for web page accessibility is complicated and unclear, the types of impairments that cause individuals problems accessing web pages are not. The following two sections will provide an overview of the impairments,

which interfere with using the web, and the solutions web designers can use to provide accessible web pages to individuals with those impairments.

HOW TO MAKE WEB PAGES ACCESSIBLE TO INDIVIDUALS WITH IMPAIRMENTS

What is accessibility? Clark (2003) suggests that accessibility "involves making allowances for characteristics a person cannot readily change." The World Wide Web Consortium's (W3C) "How People with Disabilities Use the Web" (2004) provides a number of different scenarios showing the problems people with disabilities encounter when using the web. Some example scenarios they provide are: Online shopper with color blindness; Accountant with blindness; Classroom student with dyslexia; Retiree with several aging-related conditions, managing personal finances; and Supermarket assistant with cognitive disability.

A starting point for understanding web accessibility is to examine the characteristics that interfere with an individual's ability to use web pages. These characteristics can be grouped into the following categories: Visual, Auditory, Mobility and Cognitive impairments. Visual impairment can range from complete blindness to less impaired being able to read large text on a monitor. This category should also include that significant portion of the population that has some sort of color vision problem. Auditory impairment can range from having difficulty hearing different frequencies, difficulty hearing over background noise, to complete deafness. Mobility impairment refers not to the ability to move around, but impairments that cause difficulty – or make impossible – the use of a computer keyboard and/or mouse. Cognitive impairments concern an individual's ability to process and understand the content of a web page.

Clearly these categories cover a very wide variety of physical and mental impairments. How is it possible to make a web page accessible to individuals who may be blind, deaf, unable to use a mouse, and/or have a learning disability. The solution very often requires the combination of an assistive technology and web pages that are designed to not interfere with that technology. Assistive technologies used for web access include screen readers, alternative keyboards or switches, Braille and refreshable Braille, scanning software, screen magnifiers, speech recognition, speech synthesis, text browsers and voice browsers (W3C, 2004).

Perhaps the most technologically challenging impairment to overcome for accessible web pages is blindness. To make web pages accessible to blind individuals requires both the assistive technology of screen readers and web pages

that are designed to make it easy for screen readers to do their job. The web creator's challenge is to create the web page in a way that makes it as easy as possible for someone using a screen reader to understand the content of a web page. The difficulty is that screen readers are sequential – they start at the beginning of the HTML file and read to the end. However, users who do not require screen readers are accustomed to glancing in the left column of a page to find navigation links and perhaps the right columns for navigations links also. Our eyes are capable of saving a great deal of time by not reading everything sequentially and web pages that utilize good graphical design principles are designed to take advantage of this. There are a number of approaches to making web pages that are easy to use and navigate for both sighted and blind visitors. They are not necessarily enormously complicated, but they do require an understanding of how screen readers work and things to avoid if you want the screen reader to be effective. Using HTML tables for page layout is a very widely used approach to a visually well-organized page, but can make it very difficult and tedious for a blind user to use a web page. HTML Frames and complicated JavaScript menus can also cause problems for screen readers. While it is certainly possible to retrofit solutions to these problems into an existing web page, it is much less expensive to create a new web page with these constraints in mind.

Moderate visual impairment means that the person will not need a screen reader, but rather just needs to be able to increase the size of the text to make it readable to him/her. This may involve the assistive technology of a screen magnifier or simply increasing the text font size of the page. How difficult this is depends on how the web page creator set the font sizes on the page. The preferred method is the use of relative sizes such as Medium, Small, Large, etc. The advantage of this approach is that it is interpreted in terms of the base font size set by the person. A person with a visual impairment would set their base font to be a very large one, and then these relative sizes would be in relation to that. Unfortunately, it is possible to set the font size using an absolute measure, for example twelve pixels. This makes it more difficult for the viewer of the page to increase the size of the font.

Another barrier to both moderately impaired and blind viewers is the use of images to show text. This use is understandable from a graphics design viewpoint: HTML's ability to handle text fonts is limited and dependent on whatever fonts the viewer has installed on their computer. One way around this for the designer is to use the font they want, save it as an image file and then use the image file on the page. This generally results in a very visually attractive web page, but a text reader must have text to read – it cannot read an image. The workaround to this is to set

the ALT tag of the image to describe what the image is for the screen reader to read. This is useful for images that just convey information, less useful for images that are buttons, and not at all useful for complex image maps that do different things depending where on the image you click. This is also a good example of something that is much easier to do while creating the web page, rather than having to go back and add ALT tags to all the images on an existing web page.

Color blindness is another vision impairment that results in the individual having difficulty distinguishing some colors and differentiating between two colors. The accessibility solution to this impairment does not require an assistive technology; it just requires an understanding of the problem. Once the problem is understood, the web creator can avoid using only color to convey information and be aware of particular color combinations that are difficult for many color blind individuals to see. To help with this, there are tools on the web that will allow you to see how a web page would appear to an individual with color blindness (Vischeck).

Because the web is so text and visually oriented, many web pages can be viewed by individuals with an auditory impairment with no assistive technology or specific design at all. However, if a site is presenting online videos with sound then there must be a means for providing an equivalent text version of the audio if hearing impaired individuals are to access the information contained in the audio.

Mobility impairments make it difficult or impossible for an individual to use a mouse or keyboard. Mobility impairments can include can include weakness, limitations of muscular control (such as involuntary movements, lack of coordination, or paralysis), limitations of sensation, joint problems, or missing limbs. (W3C, 2004). Assistive technologies to overcome these impairments include specialized keyboard layouts, large trackballs, various pointing devices and voice recognition software. The primary approach to making web pages accessible to this population is to design web pages that can be navigated without a mouse. There are a number of methods for doing this, but the first step is the awareness that not all visitors to your website will be able to use a mouse.

Cognitive impairments is a broad category revolving around the difficulty of processing the content of the web page. Examples of cognitive impairments are Dyslexia, Attention Deficit Disorder, Intellectual impairments, Memory impairments and Aging-Related conditions (W3C, 2004). Approaches that web creators can use to make their web pages more accessible to this population are insuring the content of the page is clear and easy to read, minimizing or eliminating distracting animations on the page and providing non-text alternative versions of the

content. An example of a non-text alternative would be an audio file of the of the web page content being read aloud.

As has been shown, there are a very wide range of visual, auditory, mobility and cognitive impairments, which can present a barrier to using a web page. It is important to note that despite the wide range of impairments it is possible to create web pages that can be used by all of these different populations, but many web page creators are not only not aware of how to create accessible web pages, they are not really aware of the fact that disabled individuals might need to view their web pages. This lack of awareness of the problems faced by impaired web viewers leads to the creation of web pages that make it very difficult or impossible for disabled visitors to use the web. The awareness and acceptance of this as a real problem to be dealt with and the willingness (and access to) training in the skills needed are the steps that creators of web pages must take to create accessible web pages.

WHY IS THIS A PARTICULARLY DIFFICULT PROBLEM FOR UNIVERSITIES

The previous section provided an overview of the types of impairments that cause difficulties for individuals accessing web pages and examples of how web creators can overcome those difficulties. A basic lesson suggested for planners is that it is much less costly to build the accessibility into new pages than to retrofit it into existing pages. Although universities have very large web sites, many corporations have very large websites also. What is it about university pages that make the goal of accessibility particularly difficult to achieve? The answer to this question lies with a combination of the de-centralized technology architecture behind the web and the unique organizational characteristics of the modern university.

The de-centralized architecture of the web means that as long as you have a computer that is running web server software and is connected to the Internet, you can publish your web pages. In a corporate setting, this factor is not typically that important because corporations tend to (wisely) feel that web pages are part of their brand image and need to be managed as such. Typically all company web pages will be hosted on one server (a computer running web server software). So the web server that represents the company's Internet domain name (i.e., acme.com), is typically one computer and most or all of the company web pages will physically reside on that computer.

The situation is quite different in a typical university setting. The difference starts with what an Internet name means in a university setting versus in the corporate world. A university Internet name (i.e., wcu.edu) very rarely represents one individual computer. Instead it represents a network of hundreds or thousands of computers. Only a small percentage of those computers will be used as web servers, but any of them could be.

The next factor is the control of the web server(s). In a corporate setting the IT group would typically have control over the web server and grant permissions to web creators on a strictly controlled, as-needed basis. Again, this is very different than a university setting where computers are controlled by administrative groups, colleges, schools, departments, programs, instructors and sometimes students, rather than the university IT group.

This de-centralized control of university web pages has allowed a great deal of flexibility for university web page creators to publish their web pages. However, the downside is that it also makes it very difficult for university planners to know how many web pages are currently published that have a university affiliation. Not only does the central IT group not control many of these computers, there is unlikely to even be an inventory of the servers and who does control them.

In a corporate setting there will often be a number of individuals and departments in the company that create and control the web pages. This may be a large number of people for a large website, but it is a finite, known list, and somebody who oversees the entire website should have that list. So if an accessibility planner wanted to check on the number of company web pages that are accessible, they would simply contact the people on that list. While not necessarily an easy or quick process, it is one that is quite possible to perform.

As previously noted, this scenario is absolutely not typical of a university situation. From the small team of professional developers working in the admissions office to create online applications, to the part-time student workers creating departmental web pages, to the full-time and adjunct faculty putting an increasing amount of course related material and content up on the web, widely disparate groups and individuals have created a phenomenal number of web pages – often with no awareness of other groups on campus, minimal to no oversight by university technology administration or legal counsel, and frequently with little or no awareness of legal/ethical concerns such as the need to make their web pages available to people with disabilities.

So while the task of inventorying a typical corporate website and guaranteeing that the web pages in it are accessible is not necessarily an easy, quick

or costless task, it is possible. As has been shown, the same process for all pages that have some sort of university affiliation could be essentially impossible, particularly in the short-term.

SUMMARY OF SITUATION FACING UNIVERSITY ACCESSIBILITY PLANNERS

Currently it is unclear whether or not universities are legally required to make their web pages accessible. If the state in which the university is located has no state legislation governing accessibility requirements, then it is possible that the university, whether it is public or private, is not currently legally obligated to ensure the accessibility of its web pages. Sovereign immunity may insulate state universities from lawsuits under Titles I & II of the ADA, while the websites of private institutions may not be considered places of public accommodation under Title III. Nevertheless, while these questions have yet to be decided, along with compliance requirements for recipients of federal funding, query whether or not it would be wise for any university, public or private, to litigate these issues, arguing that they do not have to provide equal access to the disabled in this increasingly important forum for delivering instruction. Perhaps then, a more important inquiry for technology managers, as they look to the future, is whether or not the need for accessible web pages is likely to lessen or disappear. There are a number of factors that seem to indicate that the answer to this question is a strong, *No!*

First, overall use of the web continues to rise and individuals with disabilities will lose access to important information and resources if they are not able to use the web. One report suggests that the web has "become the 'new normal' in the American way of life; those who don't go online constitute an ever-shrinking minority." (PEW, 2005). The same report suggest that while sixty-three percent of American adults now use the internet, only thirty eight percent of those with disabilities do so.

Second, there is no reason to believe that the number of traditional age students with disabilities will decline in the near future. In fact, given the current increase in the overall number of students graduating high school, if the percentage of disabled students remains constant, then the number of disabled students in the traditional age range will increase.

Third, there is a growing population of web users who do not (yet) fit into the disabled category, but share many of the impairments and hence difficulties in accessing the web. This is the aging baby boomer population, which increasingly

will experience some visual, auditory, mobility or cognitive impairment, which will impact their ability to use the web. In "Web Accessibility: A Broader View" the researchers suggest broadening the focus of accessibility to include an aging population with free time, discretionary income and an interest using the web (Richards and Hanson, 2004).

Finally, as web-based distance education courses become increasingly standard for universities to offer, the ability of disabled groups to take such courses hinges on the web pages being accessible to them. This will be a growing concern for traditional-age students who take some of their courses on-line, non-traditional, working students want to be able to take courses while working, as well as retirees who decide to return to school for additional courses. In addition to the likelihood of web accessibility becoming a greater issue in the near future, another important factor for planners is the fact that building accessibility into new pages is much less costly than retrofitting accessibility into existing, non-accessible web pages.

IMPLICATIONS FOR UNIVERSITY TECHNOLOGY PLANNERS

It is clear that the need to create web pages that are accessible to all students is not going to go away and seems likely to increase over time. To deal with this situation, university technology planners should view this as a long-term issue that is going to require developing long-term plans to address. An excellent resource for beginning this process is provided by the W3C (2002).

The first step should be to raise the awareness of all university web page creators about what accessible web pages mean and why that is important. There are still many people creating web pages, who have very little awareness of the problems impaired web users face daily. Unless the web page creator personally knows someone, who has experienced difficulty with the web due to an impairment, it is quite possible that they have no awareness of this problem. So the most important first step is to develop and implement a plan to remedy this lack of awareness.

The next step is to develop and begin implementing a long-term training plan for all university web page creators. This plan must recognize the wide variety of web creators in a university setting and approach the training of each group differently. A good starting point would be categorize university web creators into three groups: university staff, faculty and students.

University staff will probably the easiest group to reach. Both accessibility awareness training and accessible web page construction can be incorporated into

existing staff training. Part of this process should be identifying all university staff, who are web creators, and documenting the training they receive. This process will also allow a next step of documenting which pages they create, and of determining whether or not they are accessible. This is not a trivial undertaking, but as a critical mass of staff understands the problem, it will become the norm that all new pages created will be accessible, and a priority plan will be developed for retrofitting existing pages. It is important to note that one of the targets of increasing awareness of the need to create accessible web pages are the managers of the web page creators. It will be the managers (and their managers) who must sign off on the increased time and expense, which will be required to both train the web creators and to create accessible web pages. So in order for this process to work, the very highest level university administrators need to be aware of the accessibility problem and agree to work to commit the resources necessary to solve it.

Faculty will be a more difficult group to reach. But again, the first step should be building an awareness of the problem. This can be done by offering training seminars to faculty, including an accessibility segment in orientation for new faculty, and training the support staff, who help to train faculty to create web pages. In addition training should also go through the traditional channel of building awareness of deans, who help build awareness of department heads, who then understand the value of this training for their faculty. Realistically, this should be viewed as a long-term effort. Very few professors will be opposed to creating accessible web pages, but unless they have experienced working with a student with a disability and understand the problems disabled students face, faculty may be resistant to spending time on this effort – simply because they don't see the relevance of it to their classes. This is where the efforts to build faculty awareness of the problem will be vital.

Student web page creators will also be a difficult group to reach because it is a group with frequent turnover and there is typically no existing process for student training (outside of classes they take). To address this, ideally somewhere at the university there should be a class on creating accessible web pages and other training opportunities should be made available to student web page creators.

CONCLUSION

The need to create accessible web pages is a problem for universities that is unlikely to go away. In fact, it seems much more likely to present significant problems in the near future to universities that fail to react and prepare for a

population, which will increasingly demand that all web pages be accessible to disabled populations. As shown earlier, there are solutions to make web pages accessible to disabled individuals, but they have a cost. An important role for university technology planners is to build an awareness of this problem, convince administrators, staff, faculty and students that it is a real problem that must be addressed and build and implement plans for providing the training needed so that all university web page creators can create web pages that will be accessible to disabled individuals.

REFERENCES

Access Now, Inc v. Southwest Airlines, Co. (2002). United States District Court for the Southern District of Florida, 227 F. Supp.2d 1312.

Board of Trustees of the University of Alabama v. Garrett (2001). United States Supreme Court, 531 U.S. 356.

Bragdon v. Abbott (1998). United States Supreme Court, 524 U.S. 624.

Burgdorf, R.L., Jr. (1991). The Americans with Disabilities Act: Analysis and Implications of a Second-Generation Civil Rights Statute. *Harvard. Civil Rights-Civil Liberties Law Review, 26*, 413.

Carparts Dist. Ctr., Inc. v. Automotive Wholesaler's Assoc. New England. (1994). United States Court of Appeals for the First Circuit, 37 F.3d 12.

Clark, J. (2003). *Building Accessible Websites*. Indianapolis, IN: New Riders Publishing.

Doe v. Mutual of Omaha Ins. Co. (1999). United States Court of Appeals for the Seventh Circuit, 179 F.3d 557.

Eyer, K. (2005). Rehabilitation Act Redux. *Yale Law and Policy Review, 23*, 271-311.

Ford v. Schering-Plough Corp. (1998). United States Court of Appeals for the Third Circuit, 145 F.3d 612.

Grady, J & Ohlin, J.B. (2004). The Application of Title III of the ADA to Sport Web Sites. *Journal of Legal Aspect of Sport*, *14*, 145-159.

Hammond, A.S. (2003). Reflections on the Myth of Icarus in the Age of Information. *Santa Clara Computer and High Technology Law Journal*, *19*, 407-456.

Horvath, S.A. (2004). Disentangling the Eleventh Amendment and the Americans with Disabilities Act: Alternative Remedies for State-Initiated Disability Discrimination Under Title I and Title II. *University of Illinois Law Review, 2004*, 231-265.

Karlan, P.S. & Rutherglen, G. (1996). Disabilities, Discrimination, and Reasonable Accommodation. *Duke Law Journal, 46*, 1-41.

Kennard, W.E., & Lyle, E.E. (2001). With Freedom Comes Responsibility: Ensuring That the Next Generation of Technologies Is Accessible, Usable and Affordable. *CommLaw Conspectus*, *10*, 5-22.

Kiedrowski, C.L. (2001). The Applicability of the ADA to Private Internet Web Sites. *Cleveland State Law Review, 49*, 720-747.

King, N.J. (2003). Website Access for Customers with Disabilities: Can We Get There From Here? *UCLA Journal of Law & Technology*, *2003*, 6-288.

Konkright, K.E. (2001). An Analysis of the Applicability of Title III of the Americans with Disabilities Act to Private Internet Access Providers. *Idaho Law Review*, *37*, 713-746.

Locke, S.S. (1997). The Incredible Shrinking Protected Class: Redefining the Scope of Disability Under the Americans with Disabilities Act. *University of Colorado Law Review, 68*, 107-146.

Lynch, W. (2004). The Application of Title III of the Americans with Disabilities Act of 1990 to the Internet: Proper E-Planning Prevents Poor E-Performance. *CommLaw Conspectus, 12*, 245-263.

Maroney, P. (2000). The Wrong Tool for the Right Job: Are Commercial Websites Places of Public Accommodation Under the Americans with Disabilities Act of 1990? *Vanderbilt Journal of Entertainment Law & Practice, 2*, 191-204.

Martin v. PGA Tour, Inc. (2001). United States Supreme Court, 532 U.S. 661.

Mayerson, A.B. (1997). Restoring Regard for the "Regarded As" Prong: Giving Effect to Congressional Intent. *Villanova Law Review, 42*, 587-612.

McLawhorn, L. (2001). Leveling the Accessibility Playing Field: Section 508 of the Rehabilitation Act. *North Carolina Journal of Law & Technology*, *3*, 63-100.

Moberly, R. E. (2004). The Americans with Disabilities Act in Cyberspace: Applying the "Nexus" Approach to Private Internet Websites. *Mercer Law Review*, *55*, 963-999.

Myers, E. L. III. (2004). Disability and Technology. *Montana Law Review*, *65*, 289-307.

Nevada Dept. of Human Resources v. Hibbs. (2003). United States Supreme Court, 123 S. Ct. 1972.

Pallozzi v. Allstate Life Ins. Co. (1999). United States Court of Appeals for the Second Circuit, 198 F.3d 28.

Parker v. Metropolitan Life Insurance Co. (1997). United States Court of Appeals for the Sixth Circuit, 121 F.3d 1006.

PEW Internet and American Life Project. (2005). A Decade of Adoption: How the internet has woven itself into American life. Retrieved March 1, 2005 from http://www.pewinternet.org/PPF/r/148/report_display.asp

Poynter, L. (2003). Setting the Standard: Section 508 Could Have an Impact on Private Sector Web Sites Through the Americans with Disabilities Act. *Georgia State University Law Review*, *19*, 1197-1226.

Quinn, J. (November 2, 1999). Management and Technology, *New York Law Journal,* 5.

Ranen, J.S. (2002). Was Blind But Now I See: The Argument for ADA Applicability to the Internet. *Boston College Third World Law Journal*, *22*, 389-418.

Rendon v. Valley Crest Prods., Ltd. (2002). United States Court of Appeals for the Eleventh Circuit, 294 F.3d 1279.

Rich, R.F., & Erb, C.T., & Rich, R.A. (2002). Critical Legal and Policy Issues for People with Disabilities. *DePaul Journal of Health Care Law*, *6*, 1-53.

Robertson, C.B. (2001). Providing Access to the Future: How the Americans with Disabilities Act Can Remove Barriers in Cyberspace. *Denver University Law Review*, *79,* 199-227.

Roy. S. (October 2004). Suits Against States: What to Know About the 11th Amendment. *Arizona Attorney, 41*, 18-26.

Simmons, T. (2000). Working With the ADA's "Regarded as" Definition of a Disability. *Texas Forum on Civil Liberties and Civil Rights, 5*, 27-79.

Sloan, M. (2001). Web Accessibility and the DDA. *Journal of Information Law and Technology, 2*.

Student Note (November 2004). State Sovereign Immunity-Congress's Enforcement Power Under Section 5 of the Fourteenth Amendment. *Harvard Law Review, 118*, 258-268.

Sutter, L. (2000). The Americans with Disabilities Act of 1990: A Road Now Too Narrow. *University of Arkansas at Little Rock Law Review, 22*, 161.

Sweeney, D. (August 2000). ADA Fed Struggles With Web Accessibility; States Take Action. *E-Commerce, 17*(4), 1.

Taylor, P. (2001). The Americans with Disabilities Act and the Internet. *Boston University Journal of Science and Technology Law, 7*, 26-51.

Tennessee v. Lane. (2004). United States Supreme Court, 541 U.S. 509.

United States v. Playboy Entertainment Group, Inc. (2000). United States Supreme Court, 529 U.S. 803.

Vischeck, Tool for viewing web page with simulated color blindness. Retrieved March 2, 2005 from http://www.vischeck.com/vischeck/vischeckURL.php

W3C (1999). Web Content Accessibility Guidelines 1.0. Retrieved March 2, 2005 from http://www.w3.org/TR/WCAG10/

W3C (2002). Developing Organizational Policies on Web Accessibility. Retrieved March 4, 2005 from http://www.w3.org/WAI/impl/pol.html

W3C (2004). How People with Disabilities Use the Web. Retrieved March 3, 2005 from http://www.w3.org/WAI/EO/Drafts/PWD-Use-Web/

Waddell, C.D. (August 25, 2000). Will National Federation of the Blind renew their ADA Web Complaint against AOL? *Disability Compliance Bulletin, 18*(5).

Wehman, P. (1993). The ADA Mandate for Social Change.

Wisconsin v. Yoder (1972). United States Supreme Court, 406 U.S. 205.

Zappa, J.M. (1991). The Americans with Disabilities Act of 1990: Improving Judicial Determinations of Whether an Individual is "Substantially Limited". *Minnesota Law Review, 75*, 1303-1337.

TYPOSQUATTING – AN INNOVATIVE BUSINESS PRACTICE: THE LAW DOES NOT AGREE

Brian McNamara, California State University, Bakersfield
Donavan Ropp, California State University, Bakersfield
Henry Lowenstein, California State University, Bakersfield

ABSTRACT

The primary objective of this article is to address harmonizing business practices with traditional legal practices and current government regulatory initiatives as applied to Internet Law in resolving business disputes relating to "typosquatting." The law has determined that typosquatting is illegal. But is the practice of typosquatting just being overly competitive? Is the law being reactive and restrictive and flying in the face of the free-market system? This basic principle will be reviewed. This article will briefly cover cybersquatting. Typosquatting will be more closely defined. A scenario will be presented and current law applied. In arguendo, the alternative argument to current law will be presented.

INTRODUCTION

The Internet, used as a tool and technology within the commercial world, has dramatically altered traditional approaches in conducting business transactions, both locally and globally. The dynamics of these evolutionary trends are significantly redefining and refocusing on new sets of skills and core competencies. The Internet creates an environment where networking and interdependent actions are encouraged; where an interlocking series of relationships among customers, employees, distributors, suppliers, business partners, etc., are cultivated; where business entities form linkages with associated and interrelated enterprises that address issues pertaining to commonalities, complementarities, externalities, and infrastructure; where such linkages join forces that create new opportunities by enhancing productivity through establishing increased capacity, added value, and productivity.

The fact is that the Internet is not going away. It is here to stay, and then some. It is a factor we must live with and accept in the business community. Pertinent insights to this line of reasoning has been expressed by Michael Dertouzos, Director of the MIT Laboratory for Computer Science (home of the World Wide Web and birthplace of many of the high-tech products and processes that surround us today), for over two decades in predicting today's world of information with stunning accuracy (Dertouzos, 1997). Additional insights into core competencies and their corresponding skills in times of change are addressed by Hellriegel, Slocum, and Woodman in the eighth edition of their text on organizational behavior (Hellriegal, Slocum & Woodman, 1998).

The Internet poses an exciting challenge to business and commercial law. Answers to this challenge must transition with the demands of an evolving Internet as a medium for doing business, social norms, and legal evolution. Historically, business generally does well where levels of "uncertainty" are reasonable, when there is stability, predictability, and continuity in the law and how disputes are resolved; all in the interests of containing business risk. With traditional methods of doing business the usual and customary common law and the principles of free enterprise system have worked in harmony.

Regarding Internet law, it is not surprising to find legal issues have become controversial as to the rights, obligations and limits of the free enterprise system in business. This is so because the Internet as a medium for doing business provides a truly global market that includes numerous cultures and, many times, extreme diversity. In the not too distant future a high percentage of the world's population will be potential customers. Moreover, its reach is not subject to traditional legal jurisdictional lines of demarcation. No one nation of legal authority can ultimately control it, though aspects of the subject to some legal restraints.

A current study predicts that "Online retail sales in the US are expected to more than double in the next six years, reaching an estimated $316 billion by 2010. E-commerce growth will account for 12 percent of total retail sales in 2010, which would be an increase from 7 percent in 2004," according to a report from Forrester Research, Inc. (Park, 2004)

Against this backdrop business is concerned about false and deceptive acts in commerce (particularly advertising). Congress and several state legislatures, in reaction to a litany of abusive and unfair business practices, have enacted laws that are designed to stop or the very least restrict unfair business practices on the Internet. In addition, the U.S. Federal Trade Commission faces a major challenge adapting 19th

and early 20th century anti-trust/commercial law into the development of administrative rule making and enforcement of questionable electronic trade practices.

Issues of the Internet business/legal relationship will be a recurring theme throughout this article. Typosquatting is one such issue. This article will look at this subject as it relates to Internet business. The main issue in this article is to challenge the notion that typosquatting is an unfair business practice. The law has determined that typosquatting is illegal. But is the practice of typosquatting just being overly competitive? Is the law being reactive and restrictive and flying in the face of the free-market system? This basic principle will be reviewed. This article will briefly cover cybersquatting. Typosquatting will be more closely defined. A scenario will be presented and current law applied. In arguendo, the alternative argument to current law will be presented.

DEFINING THE PROBLEM

Forgetting for a moment that one can cut and paste a uniform resource locator (URL) into your Web Browser or click on a hyperlink to get to where one wants to go on the World Wide Web there is another way and that is simply typing-in the URL. It may seem old fashioned, but it has created a problem for the Internet. The concern lies in a user's inability to type correctly. For example, the user hits the key next to the one originally intended or transposes two letters instead. One my say that it is "no-big-deal" really; just type the URL over again, that is if you catch the error before clicking the GO key. If you do not catch it then you go to a web site, but not the one you intended. So what?

Disingenuous websites have been created to prey on the frailties of human error to drive visitors to their own site. Usually these websites are variations of popular websites. This practice of preying on a user's inability to type correctly has been given a name: "typosquatting." No area of the Internet has been safe from this type of practice. A simple explanation of the term is that it involves purchasing a domain name that is a variation of an original/existing popular domain name with the expectation that the new site will receive traffic off the original/existing site because of a user's misspelling of the original domain name. As an example, a typosquatter might register the domain name "www.yahooo.com" in the hopes that someone making a typo will unexpectedly log onto the typosquatter's site.

CYBERSQUATTING

Cybersquatting

As previously discussed, "cybersquatting" is loosely defined as using a name belonging to another as the URL domain address without legitimate approval or licensing from the apparent owner. The definition of cybersquatting in this instance follows the reasoning of the court in Toys "R" Us, Inc. v. Eli Abir, 1997, that describes and defines a typical cybersquatting situation. Controversies relating to domain address use were unknown a few years ago. Now, it is an integral part of our personal and business life as we conduct commercial transactions over the Internet. In short, a definition for cybersquatting is as follows: "Cybersquatting is the act of registering a popular Internet address--usually a company name--with the intent of selling it to its rightful owner." (Webopedia/cybersquatting, 2005)

TYPOSQUATTING

Typosquatting is a specific form of cybersquatting. The current definition for typosquatting is: "Purchasing a domain name that is a variation on a popular domain name with the expectation that the site will get traffic off of the original sight because of a user's misspelling of the name. (Webopedia/typosquatting, 2005). For example, registering the domain names webapedia.com or yahooo.com in the hopes that someone making a typo will get to that site unexpectedly."

Initially the typosquatters finds websites that have heavy volume of hits. The typosquatter then registers domain names that are similar to the legitimate website but have typographical errors. The typosquatter has to be creative and insightful to generate a typographical variation of the legitimate domain name that has a high probability of being typed. These tend to fall into three categories:

1. Common misspelling of the intended site; for example, webadress.com.

2. A misspelling based on typing errors; for example, wwebaddress.com or wwbaddress.com.

3. A differently phrased domain name; for example, web-address.com. (Grohals, 2005)

The typosquatter plays the numbers game that a user will mistype a popular high volume URL. When the user arrives at the unintended site several scenarios develop. The unintended site may have a competing product, it might be a pornographic site or the most irksome for a user is being mousetrapped. Mousetrapping is when someone misspells a domain name and they are then led to a series of pop up advertisements that prevent them from getting out of the Web site they originally accessed. (Webopedia/mousetrapping, 2005). To prevent mousetrapping a user needs a pop-up blocker to accomplish the task or in the worst case the user needs to shut down their computer and reboot.

The typosquatter makes money by selling advertising or by offering a related product. It is easy to see that typosquatting the high volume legitimate sites will have the best return on investment. Studies have estimated that 10 percent to 20 percent of all hand-entered URLs are mistyped adding up to at least 20 million wrong numbers per day. (Gibbs, 2003). It is easy to do the math to see that one could earn a good income in this manner. John Zuccarini one of the best-known typosquatters has registered over 3,000 typos of popular websites and generates over a million bucks a year. (Boutin, 2005).

WHAT HAS THE LAW DONE ABOUT TYPOSQUATTING?

Is this activity illegal? The law says yes. There are two ways to challenge the activity of typosquatting; 1) The Uniform Domain Name Resolution Policy (UDRP) and 2) use of the courts, in particular, the Anti-Cybersquatting Consumer Protection Act. (ACPA)

THE UNIFORM DOMAIN NAME RESOLUTION POLICY (UDRP)

The UDRP is an administrative body designed to allow victims of cyberpiracy to have their case heard quickly and with little cost. If the alleged victim is successful then the URDP recommends having the offending domain name cancelled or transferred.

In order that the UDRP administrative body finds in favor of the complainant they have to prove the following that:

(i) The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;

(ii) That the registered party (respondent) has no rights or legitimate interests in respect of the domain name; and

(iii) The domain name has been registered and is being used in bad faith. (Uniform Domain Name Dispute Resolution Policy, 1999).

It must be recognized immediately that the decision of this committee is not binding on the courts. The remedies available to UDRP are limited to transferring or canceling the offending domain name.

THE UDRP IN ACTION

The World Intellectual Property Organization (WIPO) administered a UDRP hearing involving JK Rowling (complainant), author of the popular Harry Potter book series, and Alvaro Collazo of Colonia, Uruguay (respondent.) The domain names in question were www.jkrowling.com belonging to Ms. Rowling and www.kjkrowling.com and www-jkrowling.com legitimately belonging to Mr. Collazo. By mistakenly going to these sites the user was bombarded with pop-up adds. (Scotland on Sunday, 2004).

At the hearing Mr. Collazo offered no evidence or defense. The committee confirmed that Mr. Collazo had tried to profit from Ms. Rowling's world wide fame. In reaching their decision the committee took into account the fame of Ms. Rowling, the use of the disputed website names, the similarity of the web addresses created a confusing similarity with the trademark and Mr. Collazo's pattern of conduct. The panel found that on the balance of probabilities, the disputed website names were registered and used in bad faith. The committee ordered both domain names transferred to Ms. Rowling. (WIPO Arbitration and Mediation Center, 2004)

ANTI-CYBERSQUATTING CONSUMER PROTECTION ACT (ACAP)

The court system offers an alternative to the UDRP arbitration process. However, it generally takes a long time and is generally very expensive. The key, if an alleged victim takes this avenue, is to obtain a temporary restraining order as soon as possible. In the long run, if successful, the plaintiff can obtain an injunction, damages, and/or attorneys' fees

Companies and organizations holding trademarks can allege traditional trademark claims and trademark dilution claims under the Federal Trademark Dilution Act. Once again these avenues are costly and expensive. (Karyn, 2003)

In terms of typosquatting the courts have held typosquatters liable under the Anticybersquatting Consumer Protection Act. (Shields v. Zuccarini, 2001and Electronics Boutique v. Zuccarini, 2002)

This act is an amendment to Section 43 of the Trademark Act of 1946. This act makes a person acting in bad faith who takes the name of a person or entity that has a trademark (name) liable civilly for damages incurred as a result of the taking. The act includes nine factors in determining bad faith. In Virtual Works, Inc. v. Volkswagen of America, Inc., the court enjoined the plaintiff Internet service provider from using the domain name of VW.NET, which it had registered with Network Solutions, Inc. in 1996. The owners of the site used it for their business and had intended to sell the site to Volkswagen, the owner of the VW trademark, for a substantial amount of money. With this there was a finding of bad faith. (*Virtual Works, Inc. v. Volkswagen of America,* 2000)

The ACPA conducts a 3 prong analysis on the evidence presented by the parties:

Prong 1: Under § 1125(d)(1)(A)(ii)(I) and (II), the district court first has to determine if plaintiff's domain name is a "distinctive" or "famous" mark and, therefore, is entitled to protection under the Act. The following factors may be considered when making this inquiry:

(A) the degree of inherent or acquired distinctiveness of the mark;

(B) the duration and extent of use of the mark in connection with the goods or services with which the mark is used;

(C) the duration and extent of advertising and publicity of the mark;
(D) the geographical extent of the trading area in which the mark is used;
(E) the channels of trade for the goods or services with which the mark is used;
(F) the degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom the injunction is sought;
(G) the nature and extent of use of the same or similar marks by third parties.

Prong 2: Under the Act, the next inquiry is whether Respondent's domain names are "identical or confusingly similar" to Plaintiff's mark.

Prong 3: The final inquiry under the ACPA is whether Defendant acted with bad faith intent to profit from Plaintiff's distinctive and famous mark or whether his conduct falls under the safe harbor provision of the Act. Section 1125(d)(1)(B)(i) provide a non-exhaustive list of nine factors for us to consider when making this determination:

(I) the trademark or other intellectual property rights of the person, if any, in the domain name;
(II) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
(III) the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
(IV) the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
(V) the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the

goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;

(VI) the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

(VII) the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

(VIII) the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties; and

(IX) the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of subsection (c) (1) of this section. on with the goods or services with which the mark is used; (C) the duration and extent of advertising and publicity of the mark; (D) the geographical extent of the trading area in which the mark is used; (E) the channels of trade for the goods or services with which the mark is used; (F) the degree of recognition of the mark in the trading areas and channels of trade used by the

marks' owner and the person against whom the injunction is sought; (G) the nature and extent of use of the same or similar marks by third parties.

STATEMENT OF FACTS

The University of Nowhere (UN) has registered trademarks for the "University of Nowhere" and for the University of Nowhere "Winners," the university's sports teams. The university registered its domain name, www.un.edu, through the Internet Corporation for Assigned Names and Numbers, and its uniform resource locator (URL) address has been in operation for over ten years. The University uses its Internet site to inform the public about its highly accredited academic programs as well as its accomplishments on the sports fields. The University has been recognized as one of the top universities in the United States for many years. The University has also competed successfully for numerous NCAA titles over the years.

The University discovers that Mr. Bill M. Phast, owner and Chairman of the Board of the University of Minimum Standards of America, Inc. (UMS), is registered and using the Internet domain names of "www.ums" and "www.um.edu." Mr. Phast justifies the use of the "um" designation as being part of the acronym associated with his university. This website offers university degrees through non-traditional means. The education community generally regards UMS as a diploma mill. It should be noted that UMS is located in an industrial park in the City of Nowhere and employs three clerks.

The President of the University of Nowhere, Dr. Ima Goode, contacted Mr. Phast, who informs the University president that he has no intention of relinquishing the "www.um.edu" domain name unless the University of Nowhere pays him $10,000 and gives him two lifetime passes to all "Winner" games. Dr. Ima Goode of the University of Nowhere declines the offer and writes a letter to Mr. Phast informing him that he must stop using the "www.um.edu" domain name immediately. Mr. First responds by sending the University of Nowhere an invoice for $10,000 and two lifetime passes to "Winner" events. The cover letter to the invoice states that he will not stop using the domain name until the invoice is paid by the University of Nowhere.

At a news conference three days later, Dr. Ima Goode of the University of Nowhere stated that in her opinion the "www.um.edu" domain name used by UMS

was possibly responsible for a large number of its students transferring to UMS. When questioned later by the news media, Mr. Phast stated that such allegations by the University of Nowhere were defamatory to UMS and that the University of Nowhere has no legitimate right to the "www.um.edu" domain name since its official acronym is "UN" and not "UM." What are the issues of this case and the rights of the parties?

The arbitration panel would probably determine that University had a common law and trademark rights in University of Nowhere Winners, and that the domain names issued to Mr. Phast, the respondent, were confusingly similar to the University's trademark. Additionally, the panel would rule that Mr. Phast had no rights or legitimate interests in the domain name, and that they were registered and used in bad faith. Additionally, the respondent would have no legitimate interests in respect of the domain name where he had not used or developed the domain name for legitimate noncommercial or fair purposes and was not using the domain name in connection with a *bone fide* offering of goods or services. Lastly, the respondent, Mr. Phast, directly implied that he wanted a sum far greater than registration costs in exchange for the transfer of the four domain names. This action is a *per se* finding of bad faith. Final outcome: the University wins. What the University wins will depend on the documentation that the University originally filed. There could be deletion or transfer of the domain name.

The case would reach a similar conclusion under ACPA given their rulings to date. However, are the courts being too protective in their analysis? Consider the following applying the three pronged analysis of the ACPA.

PRONG 1 – DISTINCTIVE OR FAMOUS MARK

It is conceded that the University of Nowhere is a well-known institution recognized across he country and therefore the trademark and domain name are protected.

The first prong is met.

PRONG 2 – CONFUSINGLY SIMILAR

"A reasonable interpretation of the conduct covered by the phrase "confusingly similar" is the intentional registration of domain names that are

misspellings of distinctive or famous names, causing an Internet user who makes a slight or typing error to reach an unintended site." (Shields v. Zuccarini, 2001)

So what? Why stifle competitive business practices. Where the courts get it wrong in their analysis is that they interpret everything from the alleged wrong party and proscribe what the Internet user wants to see.

"A reasonable interpretation of the conduct covered by the phrase "confusingly similar" is the intentional registration of domain names that are misspellings of distinctive or famous names, causing an Internet user who makes a slight or typing error to reach an unintended site."

So what? Why stifle legitimate competitive business practices. The courts, in this instance, are interpreting from the perspective of the plaintiff using the analysis that everything from the alleged bad party is "guilty" until proven "not guilty" (using criminal law terms for point of clarification) and then proscribe what the Internet user wants to see.

1. The domain in question is just a geographical area on the Internet, serving to identify locations wherein the universities information can be located. The URL in and of itself is just a location and as such has no value.
2. It is the user who makes the error. The user finds um.edu not the other way around.
3. The user can decide whether they want to investigate the website further or not.
4. The degree offered at um.edu will be cheaper than the one offered at un.edu. Is it the courts' job to restrict the free-market system.
5. Insurance companies are very prosperous businesses who make money on the fact that people might make mistakes. The law does not work in this area to protect the big insurance companies from their competitors.

Giving great weight to the above, Plaintiff's fails on prong 2.

PRONG 3 – BAD FAITH

The final inquiry under the ACPA is whether Mr. First acted with bad faith intent to profit from University of Nowhere's distinctive and famous mark

So what, again? When one discusses the issue of bad faith it is implicitly understood that there exists a contract or some type of privity between the two parties, in this case the plaintiff and respondent. This concept is derived from the Uniform Commercial Code. There is no contract and no privity here so how does one determine bad faith. Why is it so hard for the courts not to appreciate the ingenious and smart moves of the businesses who registered domain names on a first come first served basis only to have their business savvy interpreted by courts declaring immediately that such actions are considered as "bad faith." Where is the chance for the respondent to respond beyond the pronouncement of being a party of bad faith and proving a legitimate commercial transaction in place of the specific action that designates bad faith intent? There is a chance somewhere that sending an invoice for a domain name is not always a bad faith action.

The factors listed to establish bad faith smell of reverse engineering. It appears the court is saying, "we want to stop this practice so lets generate a list of criteria to stop the practice." Remember Dick Fosberry? Dick Fosberry looked at the high jump in a way nobody else did. He developed a technique to do the high jump better than anyone else. He was smart, innovative, competitive and successful. The first question asked when the athletic world saw his technique was - is it legal? Lucky for the athletic world they deemed it so. Businesses should be so lucky to have the same characteristics as Dick Fosberry. Typosquatters are business people, they looked at a situation differently and profited. Why should the courts intervene? The American way is competition and the free market system.

Giving great weight to the above, Plaintiff's fails on prong 3.

CONCLUSION

There exists today a tension on the Internet between the desire to make it a safe environment to transact business. Opportunity for profit is a function of business, why should the Internet be any different. The ACPA gives the federal government the power to clamp-down on typosquatters. One hope this article makes the reader reconsider how the court is analyzing this business activity.

The perceived problems with typosquatting would go away if a business purchased all the domain names they might need before using a mark in commerce. As it currently stands there is no need to rush because the courts will protect your lack of forward thinking, insight and business competitiveness.

The explosive growth and popularity of the Internet and other developing allied technologies has proven challenging to the traditional business model. Complexities, complications, and new issues will continue to expand as the Internet and the World Wide Web evolves. Questions and concerns will continue to challenge traditional business practices in a changing global economy.

Today, there exists a myriad of issues to be resolved as to creating an Internet with a safe environment for transacting business. Opportunity for profit is a function of business, so why should the Internet be any different. The ACPA gives the federal government the power to clamp-down on typosquatters. It is time to reconsider how the court is analyzing this specific business activity. There is always a need to protect society from itself, but there is also a demanding need to conduct commercial activities.

Presently, the balance, in some instances, such as the one described in this case study, does not favor businesses. It is time for the legislatures and courts to review, adjust, and properly balance the system so as to give businesses the incentive to participate in commercializing new technology without fear of unknown restraints and undefendable per se violations. This theme was active and available for transitioning from the 18th to the 19th Century and should be available for transitioning from the 19th to the 20th Century. The essence of this article is to communicate that it is not fair to constructively judge a business person as acting in "bad faith" when there is no process of introducing what the intent of the action was from the prospective of the respondent.

REFERENCES

Boutin, P. (2005). The Typo Millionnaires. Retrieved from Webhead, February 11, 2005 from http://slate.msn.com/id/2113397#ContinueArticle.

Dertouzos, Michael (1997). What Will Be; How the New World of Information will Change our Lives, *HarperEdge.*

Electronics Boutique v. Zuccarini (2002). 33 Fed Appx. 647 (3d Cir.2002). Retrieved from http://www.keytlaw.com/Cases/electronic.htm.

Gibbs, M. (2003). The 'Net up for grabs. *Network World.* Retrieved September 22, 2003 from http://www.networkworld.com/columnists/2003/0922backspin.html.

Grohals, J. (2005). Typosquatting. Psych Central. Retrieved June 28, 2005 from http://www.psychcentral.com/psypsych/Typosquatting.

Hellriegel, Don, John W. Slocum, Jr. & Richard W. Woodman (1998). *Organizational Behavior,* Eighth Edition, South-Western College Publishing.

Karyn M. (2003). Retrieved from UNC School of Law as an assignment for a Cyberlaw Class by Professor Gasaway http://www.unc.edu/courses/2003spring/law/357c/001/projects/karyn/domainnames/Courts%20v%20UDRP.htm

Park, Roger (2004). On Line Sales Predicted to Soar. Retrieved August 27, 2004 from http://www.imediaconnection.com/content/4098.asp

Scotland on Sunday (2004). Fiona MacGregor, December 12, 2004 page 5.

Shields v. Zuccarini (2001). 254 F.3d 476 (3d Cir. 2001) retrieved from http://www.keytlaw.com/Cases/shields.htm

Toys "R" Us, Inc. v. Eli Abir (1997). 45U.S.P.Q.2d (United States District Court for the Southern District of New York), 1997.

Uniform Domain Name Dispute Resolution Policy (1999). Retrieved from http://www.icann.org/

Virtual Works, Inc. v. Volkswagen of America, Inc. (2000). 106 F. Supp. 2d 845 (E.D.Va 2000)

Webopedia/cybersquatting (2005). Retrieved from http://www.webopedia.com/TERM/C/cybersquatting.html

Webopedia/typosquatting (2005). Retrieved from http://www.webopedia.com/TERM/T/t yposquatting.html

Webopedia/mousetrapping (2005). Retrieved from http://www.webopedia.com/TERM/M/mousetrapping.html

WIPO Arbitration and Mediation Center (2004). Joanne Rowling v. Alvaro Collazo, Case No. D2004-0787. Retrieved November 22, 2004 from http://arbiter.wipo.int/domains/decisions/html/2004/d2004-0787.html.