ISSN: 1545-679X

Information Systems Education Journal

Volume 6, Number 29 http://isedj.org/6/29/ March 6, 2008

In this issue:

The Place of Cyberlaw in MSIS Curricula

Ramesh Subramanian
Quinnipiac University
Hamden, CT 06518 USA

Bruce A. White
Quinnipiac University
Hamden, CT 06518 USA

Abstract: The growth in the IT field has redefined the role of the IT manager. The furious pace of growth in global commerce facilitated by the Internet has led to greater governmental role in controlling and regulating E-commerce. Developments in technology have also led to a trend towards digitization of personal, commercial and governmental data. All of this has led to a plethora of laws, both domestic and international, that govern the use of IT. In some cases the laws are as intricate and obtrusive as to affect the research, design, development and operations of information technologies in organizations. Given this scenario, the IT manager should become more than a little aware of these laws pertaining to IT. Yet, a look at the model IT curricula reveals that not much has been done as far as the IT curriculum is concerned in this area. This paper addresses this gap and proposes the justification and design of a course in IT and the Law.

Keywords: information technology, information systems education, graduate IS curricula, cyberlaw, law, IT manager

---

Recommended Citation: Subramanian and White (2008). The Place of Cyberlaw in MSIS Curricula. *Information Systems Education Journal, 6* (29). http://isedj.org/6/29/. ISSN: 1545-679X. (Also appears in *The Proceedings of ISECON 2006:* §2355. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/6/29/**

The **Information Systems Education Journal** (ISEDJ) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1545-679X. • First issue: 8 Sep 2003. • Title: Information Systems Education Journal. Variants: IS Education Journal; ISEDJ. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@isedj.org. • Subscription price: free. • Electronic access: http://isedj.org/ • Contact person: Don Colton (editor@isedj.org)

2008 AITP Education Special Interest Group Board of Directors

Paul M. Leidig Grand Valley State University EDSIG President 2005-2006	Don Colton Brigham Young Univ Hawaii EDSIG President 2007-2008	Robert B. Sweeney U South Alabama Vice President 2007-2008
Wendy Ceccucci Quinnipiac Univ Member Svcs 2007-2008	Ronald I. Frank Pace University Director 2007-2008	Kenneth A. Grant Ryerson University Treasurer 2007-2008

Albert L. Harris Appalachian St JISE Editor	Thomas N. Janicki Univ NC Wilmington Director 2006-2009	Kevin Jetton Texas St U San Marcos Chair ISECON 2008	Kathleen M. Kelm Edgewood College Director 2007-2008

Alan R. Peslak Penn State Director 2007-2008	Steve Reames Angelo State Univ Director 2008-2009	Patricia Sendall Merrimack College Secretary 2007-2008

Information Systems Education Journal Editors

Don Colton Brigham Young University Hawaii Editor	Thomas N. Janicki Univ of North Carolina Wilmington Associate Editor

This paper was selected for inclusion in the journal as part of the ISECON 2006 best papers group. Best papers received preliminary reviews by three or more peers placing them in the top 30% of papers submitted and final reviews placing them in the top 15% by persons unconnected with the conference or the journal, and whose names are withheld to preserve their anonymity.

EDSIG activities include the publication of ISEDJ, the organization and execution of the annual ISECON conference held each fall, the publication of the Journal of Information Systems Education (JISE), and the designation and honoring of an IS Educator of the Year. • The Foundation for Information Technology Education has been the key sponsor of ISECON over the years. • The Association for Information Technology Professionals (AITP) provides the corporate umbrella under which EDSIG operates.

© Copyright 2008 EDSIG. In the spirit of academic freedom, permission is granted to make and distribute unlimited copies of this issue in its PDF or printed form, so long as the entire document is presented, and it is not modified in any substantial way.

The Place of Cyberlaw in MSIS Curricula

Ramesh Subramanian
Ramesh.subramanian@quinnipiac.edu

Bruce White
Bruce.white@quinnipiac.edu
Information Systems Management Department
Quinnipiac University
Hamden, CT 06518 USA

ABSTRACT

The growth in the IT field has redefined the role of the IT manager. The furious pace of growth in global commerce facilitated by the Internet has led to greater governmental role in controlling and regulating E-commerce. Developments in technology have also led to a trend towards digitization of personal, commercial and governmental data. All of this has led to a plethora of laws, both domestic and international, that govern the use of IT. In some cases the laws are as intricate and obtrusive as to affect the research, design, development and operations of information technologies in organizations. Given this scenario, the IT manager should become more than a little aware of these laws pertaining to IT. Yet, a look at the model IT curricula reveals that not much has been done as far as the IT curriculum is concerned in this area. This paper addresses this gap and proposes the justification and design of a course in IT and the Law.

Keywords: Information technology, Information Systems education, graduate IS curricula, cyberlaw, law, IT manager

1. INTRODUCTION

The growth of the Internet in the last two decades has redefined today's business. The Internet is indispensable today as a tool and as a platform to conduct business. This has redefined the role of the IT manager. Today, the IT manager performs multiple roles covering the entire range of the IT function, from high-level IT strategy and IT championing, to mid-level IT operations and planning, project management and sourcing management, to functional roles such as network and communications management, data management, hardware/software management, etc. – all within the overarching umbrella provided by the Internet. The MSIS model curriculum of 2006 reflect the changes affecting the IT field and the IT manager's role and suggest curriculum models that address many of the above shifts in some degree or other.

However, one area that is not adequately addressed so far in the IS model curricula is that of regulation and law affecting the IT/IS manager. The new MSIS2006 model curriculum mentions law in the new course "Implications of Digitization" course (MSIS2006.8)," but the course has many focuses (ethics, employee monitoring, compliance [like Sarbanes-Oxley], globalization and sourcing, and more. (Gorgone, et. al, 2006)." As seen here, the term "legal" is mentioned almost in passing. As IT's influence spreads to all aspects of society, it is imperative that all levels of IT managers become familiar with various regulations and laws that affect the design and functioning of IT in organizations.

In the new MSIS 2006 model curriculum for graduate MSIS programs, a track is suggested for Computer Forensics that includes a course in Criminal law and a course in Computer Forensics. But, this is part of a

listing of twenty-four representative career tracks and suggested courses.

This paper suggests a mandatory course on the legal aspects of IT/IS in the MSIS curriculum and argues that the law and its affects on IT/IS in the current environment is too crucial to be considered as simply "optional." The paper first discusses IT developments in the last two decades and the consequent increase in the need for security, privacy and regulation. Following that stream of thinking, the paper then argues for a mandatory course on IT and the law, and lists some important topics that should be included in such a course. This is followed by brief discussions on the individual topics listed earlier, along with justifications. The paper ends with a discussion on how such a course could be designed and delivered.

2. IT DEVELOPMENTS AND THE NEED FOR SECURITY, PRIVACY AND REGULATION

The last decade of the twentieth century was the decade of the Internet. The invention of the World Wide Web (Web) by Tim Berners-Lee, who built the first Web site in 1991 while working at the European Organization for Nuclear Research (or CERN) in Geneva, Switzerland started a world-wide trend in developing Web sites not only for personal and research purposes, but for disseminating governmental information and for engaging in global electronic commerce. Thus the Internet, with its "killer application," the web, heralded the furious pace of globalization in the 1990s.

As the Internet and the Web continue their furious growth and global spread, they have filtered down to encompass every aspect of society. Nowadays it is rare to see an aspect of domestic or public life that is not in some way touched by the Internet. This situation is not restricted only to the technologically developed countries, but is becoming increasingly prevalent in developing countries too. As a result, new terms and phrases such as "virtual world," "cybercrime," "computer virus," "data privacy," "identity theft" and "data mining" have entered the everyday vocabulary. Debates have ensued on the virtues and vices of the Web and the consequent large scale digitization that it has heralded. While many have argued that the pace of the growth of the Internet, the Web, E-commerce and the digitization should continue without any curbs or governmental restrictions, others have argued the exact opposite, that these should be actively regulated and controlled through laws both domestic and international. The latter group has argued that unregulated and unmitigated growth of the web coupled with the current pace of digitization of almost all data belonging to individuals could cause an erosion of privacy and cause them to become exposed to malware and identity theft. This would, they argue, curb E-commerce and seriously affect global economic development and growth. Indeed, in the 1990s the Internet was considered to be a virtual world that was ungovernable and thus could not fall under the purview of any government. Proponents of this view felt that the users of the Internet would somehow govern themselves and make it into a global vehicle of commerce and information outside of any governmental influence. However, in recent years, realizing the importance of the Internet, governments have also stepped in to flex their muscles in an attempt to gain control of the Internet through regulations and laws. Predictably, increasing government regulation of the Internet has its detractors who believe that certain fundamental rights such as the freedom of expression may be lost if the government controls the Internet. This is notwithstanding the fact that the Internet, in its nascent stage was completely funded by the US government.

Part of the reasoning behind governmental regulations is purportedly to protect citizens and business enterprises from cybercrimes, and thus protect their rights to a civil society, even though it could be argued that part of it is an to exercise control over citizens' use of the Internet. In the former case, governments have sometimes been actively supported by industry and the common citizen. In the next section we focus on the issue of cybercrime and the evolution of cyberlaw.

3. IT, CYBERCRIME AND THE LAW

The term "cyberspace" was coined by science fiction author William Gibson in his 1984 novel *Neuromancer*. "Cybercrime," which originates from the word cyberspace, is "a term used broadly to describe criminal

activity in which computers or networks are a tool, a target, or a place of criminal activity" ("Cybercrime," 2006, paragraph # 1). The explosive growth of global E-Commerce has also resulted in an equally explosive growth in cybercrimes. Criminals who once operated in real-world "terrestrial" crimes have quickly adapted to the virtual world of the Internet, taking advantage of the anonymity and transience that the Internet offers them. Cybercrime is currently a very important global issue that has the potential of adversely affecting international economics, business, trade, security and human rights. Due to the global nature of the Internet, crimes can be committed from far-away locales, making the criminal difficult to apprehend. Many lesser-developed countries do not even have adequate laws to address cybercrimes. A case in example is the "ILoveYou" virus which appeared in May 2000 and caused major disruptions and shutdowns of computers and mail servers all over the world (Symantec, 2000). The virus was eventually traced to Onel de Guzman, a Philippines national. However, the government of Philippines could not adequately prosecute de Guzman due to the lack of internet crime laws at that time and he was released soon after his arrest (Burke, 2000).

Cybercrime covers a wide swath of area, and can be categorized loosely into the following areas (adapted from "Cybercrime," 2006, paragraph 2,3,4,5):

- Computers and networks as the tools of criminal activity: E.g., spamming, IP and copyright-related crimes, crimes committed through peer-to-peer networking
- Computers and networks are the target of criminal activity: E.g. unauthorized access, denial of service, attacks using malicious code
- Computers and networks as the place of criminal activity: E.g. computer-based frauds such as financial fraud
- Computers and networks as new facilitators for older crimes: E.g. child pornography, Nigerian 419 schemes, online gambling, phishing, espionage, terrorism

In addition, Kerr (2003) categorizes computer crimes as:

- Traditional crimes committed using computers (E.g. Internet fraud schemes, Internet gambling, online distribution of child pornography and cyberstalking), and
- Crimes of computer misuse (E.g. computer hacking, distribution of worms and viruses and denial-of-service attacks).

Governments around the world have started recognizing the need for framing laws to prosecute, often across global borders, those engaged in cybercrime. Much of the new laws and agreements governing cybercrime have emerged from the technically advanced counties, namely the United States and the European Union. However, other countries have also started framing cybercrime laws. Applying these laws have not been always smooth, as international laws overlap competing and even contradictory national goals, territorial and sovereignty issues.

In summary, it is seen that in today's global business climate, knowledge about the Internet, cyberspace, cybercrimes and subsequent developments in cyberlaws should very much be part of a business manager's toolset, especially one who manages the IT resources of organizations. It is important that the future IT manager understands the basics of the legal environment and justice system of the countries he/she works in, the actual laws (especially those contextual to the Internet) that affect today's working environment, the positive and negative aspects of the laws, how these laws affect his/her functioning, how the laws differ from nation to nation – even across some States within the same nation, the repercussions that the laws can have on an individual's rights to privacy and freedom of expression and the roles of the society, government and the industry in shaping these laws.

There is thus a clear justification for an IS course in IT-related law that covers all of these aspects. Current graduate IS curricular offerings in law includes include (at most) contracts law, within the context of E-Commerce. The future IT manager should expand his/her legal toolset to include familiarity with many more laws related to handling cybercrime, privacy, constitutional guarantees, jurisdictional issues, international laws, laws pertaining to corporate accounting information and laws protecting information pertaining to individuals. In the next section we discuss the elements of a course in IT and the law.

4. A COURSE IN IT AND THE LAW

A course in IT and the Law (in an American context) should thus include but not be limited to the following topics:

1. Introduction to the American Justice System
2. Introduction to Cyberspace
3. Jurisdiction in Cyberspace
4. Computer fraud and abuse laws
5. Introduction to regulating Cyberspace
6. First Amendment and other constitutional issues
7. Copyrights and intellectual property protection
8. Privacy and encryption
9. Regulation of E-Commerce

A brief synopsis of each of these topics follows.

Topic 1: Introduction to the American Justice System

The American justice system can be generalized into two parts, one addressing criminal offenses and the other addressing civil offences. In order to prove a criminal offense three factors must be established: Actus Reus (a guilty act), Mens Rea (a guilty mind), and the appropriate circumstances. These three factors need to be proved in order to convict a defendant of a criminal act. Civil offences include torts or breach of contracts. Criminal offenses are handled by criminal law, which are of two types: – statutory and common law. Statutory law is written by legislature and ratified. Common law is refined and distinguished by the justice system itself, through precedence. Based on common law, computer fraud is still fraud – it is just executed with a different medium. As new crimes emerge, new laws may have to be enacted to address them.

The judicial power of the Federal courts "extend to cases arising under the Constitution, an act of Congress, or a treaty of the United States; cases affecting ambassadors, ministers, and consuls of foreign countries in the United States; controversies in which the U.S. government is a party; controversies between states (or their citizens) and foreign nations (or their citizens or subjects); and bankruptcy cases" (Legislative Branch, 2006).

The state governments have the greatest influence over most Americans' daily lives. Each state has its own written constitution, government, and code of laws. There are sometimes great differences in law and procedure between individual states, concerning issues such as property, crime, health, and education (State, tribe and local governments, 2006).

In the IT and the Law course, this topic will thus provide an introduction to the American justice system – how laws are framed, statutory versus common law, Federal and State laws in the US legal system, how the US Federal laws can be (and cannot be) applied in foreign countries, etc. The issue of applying US federal laws in foreign countries is especially relevant in cybercrimes where a foreign national may be perpetrating a crime within the US from abroad, and vice versa. The issue of extradition to and from the US should also be examined within this topic.

Topic 2: Introduction to Cyberspace

The motivation for this topic is not to address the technological aspects of cyberspace, even though that could be added on depending upon the background and preparation of the audience. This topic will seek to define what the notion of cyberspace is, and whether a boundary can be established for such a space using technology. The topic will also address what kinds of laws can apply on this space. The issue of who controls the Internet (and cyberspace) will also be discussed here. Controls can take several forms, from top-down controls established by national governments to bottom-up or community based controls. One issue that will gain importance in the future is the *extent* of control, and the technologies used for such controls by the government, and how those controls directly interfere with the fundamental rights of the users of cyberspace. For example, the courts, in adjudicating issues pertaining to free speech, might be interested in knowing if the government has used the "least restrictive means" to regulate speech on the Internet (Chon, 1999). This eventually becomes a legal as well as a technological issue which makes it relevant to IT professionals.

Topic 3: Jurisdiction

The issue of jurisdiction becomes very important in cyberspace. Discussion on this topic must first focus on the laws pertaining to personal jurisdiction, and then move to apply them to cyberspace. In personal jurisdiction, in order for prosecution to take place the applicable court must have jurisdiction over the parties involved. "Jurisdiction" simply means the place where the crime was initiated. This concept becomes difficult to define when the offending parties could be scattered around the country, as could happen in cybercrimes. The prosecuting court must have two types of jurisdiction over the parties for a trial to be held: subject matter and personal jurisdiction. Subject matter jurisdiction dictates which type of dispute can be brought before a particular court. Typically, state courts handle any type of lawsuit that pertains to citizens of the same state. Federal courts, on the other hand, handle lawsuits that pertain to federal laws and inter-state lawsuits. However, to complicate matters, there are certain state courts that handle cases of general jurisdiction, i.e. any sort of dispute between any parties. Federal courts thus have only limited jurisdiction. Personal jurisdiction gives the court the power to enforce judgment over specific defendants. In civil cases, the two issues are: which state does the defendant belong to, and what is the constitutional appropriateness of extending the arm of a court to reach into another state to enforce a judgment on a defendant. The first issue above suggests that the offending parties should have committed the offence in the same state. However, this is a problem when the offense is committed through a medium such as the Internet (i.e. not in the same state). The state court thus needs to have the ability to prosecute out of state offenders. The way in which they gain jurisdiction over an out of state entity is by means of the "long arm" statute. This statute allows the court to impose jurisdiction over a party that had sufficient contact with a resident of its state. What constitutes the adequate level of minimum contact is up to the individual states and is limited by the constitution. This leaves a lot to be determined before a venue can be decided. Traditional crimes (even if done over the Internet) are resolved easily. For example, if a hacker is in one state and commits fraud in another state, he/she is not only liable in the state he/she lives for hacking and fraud, but is also guilty of the same offense in the other state, and since it crossed state lines the venue could be held in federal court too. It is up to the courts to pick one of the three venues for the trial. Usually the court that has the best chance for a conviction is the chosen one. But when new cyber crimes arise that do not meet the criteria new laws need to be changed or adopted to stop these new crimes (adapted from Casey, 2004 pp42-45).

There are several other issues pertaining to jurisdiction and how the courts are adjudicating on these issues, which could be studied under this topic using current cases pertaining to cyberspace.

Topic 4: Computer fraud and abuse laws

Before the advent of the Internet, creating a virus and hacking was not classified by law. The earliest hackers belonged to the "414-gang" named after a telephone area code in Wisconsin. The 414 gang started hacking into computers from 1980 onwards, and were arrested in 1983 by the FBI after hacking into the computers of the Los Alamos National Laboratory and New York's Sloan-Kettering Cancer Center in 1982. This was the earliest case of "hacker arrest" in the US (PC World Staff, 1999). This was when the world first came to understand the threat posed by hackers. This threat spurred enactment of new laws. One of the first computer protection acts was the Computer Fraud and Abuse Act (CFAA) 1984 later revised as the CFAA 1986. The CFAA was designed to protect against malicious acts and unauthorized access. Unauthorized access under the CFAA was classified as a situation where a user exceeded the access and use rights authorized to him/her. The CFAA also addressed Denial-of-service (DOS) attacks. If the DOS attack resulted in a loss of $1000 or more the offender could be brought up on civil charges. The CFAA also stated that for a crime to be committed, simple unauthorized access was enough – there did not have to be any malicious intent. This act is the basis of all cyber crime acts that have since come into existence.

This topic would therefore examine the background and genesis of early legislation covering computer crimes and cover the

various sections of the CFAA in detail, along with illustrative cases.

Topic 5: Introduction to regulating Cyberspace

The Internet was originally conceived as a network of networks, and mostly developed by scientists in academic institutions working on US Department of Defense (DoD) funded projects. Initially the US government did not pay much attention to the issue of controlling the Internet. In the 1990s, libertarians such as John Perry Barlow and Julian Dibbell began to perceive the Internet as a virtual world which could not be controlled or stopped by governmental regulations. They lapped up the concept of a cyberspace which was a truly independent entity governed only by its users through a process of consensual self government (Goldsmith and Wu, 2006). This notion was generally supported by the engineers and scientists who designed the Internet. The government gradually became aware of the near anarchy prevailing on the Internet and made moves to establish some control over the Internet. A first salvo was fired by legislators who enacted the Communications Decency Act (CDA) in 1996, which sought to control the content of the materials transmitted over the Internet.

Several other laws and actions aimed controlling the Internet and regulating online commerce have been undertaken or enacted since then. Two important and well publicized issues on regulating the Internet pertain to peer-to-peer file sharing and unsolicited commercial email (UCE), also known as SPAM. On the other extreme, certain democratic governments are challenging the overt Internet censorship that is practiced by totalitarian China, and are using their own policies to censor, control and restrict companies that enable China to set up such censorship. This is thus an area that is going to continue seeing more laws and resistance to such laws.

Many of the laws regulating the Internet have been and continue to be challenged. For example, the CDA was promptly challenged in the courts by the Electronic Frontier Foundation (EFF) set up by John Perry Barlow along with Mitch Kapor, founder of Lotus, and John Gilmore, the first programmer at Sun Microsystems) and the American Civil Liberties Union (ACLU) (Goldsmith and Wu, 2006). Regardless of the eventual outcome of such challenges, an IT manager needs to understand the laws and the trends in governmental control of the Internet as well as the arguments against such control. This topic will thus address those issues.

Topic 6: First Amendment and other constitutional issues

This topic will explore the First Amendment freedoms of speech and press as applied to the Internet. This topic will follow the earlier discussions on regulating the Internet and the Communications Decency Act and will typically use cases as well as note cases to discuss the First Amendment to the US Constitution, which protects freedom of expression. The topic will use pornographic speech as the context to discuss the position of "cyberspeech" on the continuum that runs from a nearly total absence of government regulation (the print model) to nearly unfettered governmental discretion to regulate (the broadcast model) (Easton, 1999). This topic would also discuss the courts' application of various First Amendment doctrines – prior restraint, overbreadth, public forum, etc. – to on-line speech. Additional issues considered will include limitations on the First Amendment's power to protect speech-acts, including threats, trespass, and restraint of trade. Another issue that could be considered, again with the use of actual cases, is that of libel, focusing on Internet Service Provider liability.

Topic 7: Copyrights and intellectual property protection

The protection of intellectual property (IP) is enshrined in Article I Section 8 of the US Constitution. The US Copyright Act of 1976 grants several rights to the owner of a copyright. A copyright is automatically created if a work is an original expression that is fixed in a tangible form. With the advent of the Internet, violations of digitized data have become easy. Copyright laws have been invoked in several cases by owners of copyrights to prove that the posting of copyrighted images on public-access or subscription based web sites exceed the "fair use" doctrine (e.g. Playboy Enterprises Inc. v. Ferna, 1993). In this instance Ferna provided copyrighted images from Playboy on a member-only bulletin board which could be

downloaded by the members. In other cases, copyright laws have had to be augmented to in order to prosecute new types of copyright violations that have emerged along with the Internet. For example, in 1994 David LaMacchia of MIT was indicted for running an electronic bulletin board which aided the copying of proprietary software (United States V. LaMacchia, 1994). His case was dropped, however, because David did not charge for the use of the bulletin board. In response, the No Electronic Theft (NET) Act was passed in 1997 which removed the requirement of profit motive in prosecuting copyright violations. In the year 2000, Napster, a service that enabled members to share copyrighted music, was shut down by a federal district court, because Napster users were not engaging in personal use of the music they owned, but were trading them with thousands of strangers (Lange, 2001).

Thus we notice that laws concerning copyrights have had to change along with developments in technology. This topic will discuss the legal developments in copyright and IP protection in the context of the Internet and E-Commerce.

Topic 8: Privacy and encryption

Privacy is a tricky issue to deal with. Before the advent of technology, the right to privacy was relatively sound. An individual could expect a reasonable amount of privacy from individuals and privacy from unreasonable searches from the government (4th Amendment to the US Constitution). The common law "right to privacy" as described by Casey (2004, p51) states that,

1. Appropriation of a person's name or likeness for the defendant's benefit.
2. Unreasonable intrusion, defined as intentional interference with another person's interest in solitude and seclusion.
3. Public disclosure of private facts.
4. False light, that is, publicity which presents a person to the public in a false light.

Before the development of computers and the Internet, an individual would have to be quite intrusive to violate these common laws. So the expectation of privacy was high. The Internet is, however, a very accessible and easily available and can be used to find private information about any citizen. In California v. Greenwood (1987), Greenwood's garbage was searched upon a tip that he was operating a drug business. The trash was left on the curb and was searched without a warrant. The search of the trash turned up drug paraphernalia. With that evidence in hand, a warrant was issued for his home and a drug factory was discovered inside. He was convicted and later appealed saying it was an invasion of privacy to search the trash without a warrant and any choices made on those findings were unconstitutional. The court affirmed that there was no expectation of privacy for things left out that the public could access, and therefore privacy did not apply to the trash left for the public to see. This case is the basis for the reason why privacy is a thing of the past. This ruling is also applicable to current computer technology. *If private information is left out in a public domain it is "fair game,"* and thus loses its "private" quality. Thus, whether it is trash on the curb or a web site, it will be viewed as the same.

There are several other cases that demonstrate how the courts have started interpreting privacy in the age of the Internet. After the terrorist attacks of September 11, 2001, the US government has gained much leeway when conducting warrant-less searches, which could be considered a clear violation of a person's privacy. The USA Patriot Act of 2001 (USA Patriot Act, 2001) allows government and state entities to monitor and search to a large degree before needing a warrant. It is important for today's IT manager to understand the 'right of privacy' which is protected by common law and statutes. The word 'privacy' does not appear in the US Constitution and thus the right of privacy in this context is largely a separate body of law developed over many years through interpretations and analysis of the Fourth Amendment, which prohibits 'unreasonable searches and seizures.' The Privacy Act of 1974 (Privacy Act, 1974) attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. There is a plethora of other laws relating to privacy, such as the Health Insurance Portability and Accountability Act (HIPAA), enacted by the U.S. Congress in 1996, and the Family Edu-

cational Rights and Privacy Act of 1974 (FERPA), to name a few.

The IT manager must learn, through appropriate cases, the direction in which the American legal system is going as regards privacy rights.

Topic 9: Regulation of E-Commerce

Electronic commerce, which has enjoyed a rapid rise since the advent of the Web, raises many interesting questions pertaining to the binding legality of business transactions. In the real world business transactions are controlled by contracts law. This typically assumes that a transaction takes place between two entities, and issues could rise about the price, the nature and condition of the goods purchased, and the entities concerned. These problems are handled by contracts law. But in the situation becomes more complex when a business transaction between two entities takes place in cyberspace. Typically the entities do not meet each other, and transact their business in the relative obscurity and privacy of cyberspace. The transaction itself may involve many jurisdictions. Issues such as the legalities affecting types of products or entities that could be exchanged or traded, and arguments about "pulling" a good from the Internet versus "pushing" a good on t the Internet could become important. The performance, quality, and legality of goods purchased online, and enforceability of general contracts law to these goods could also become questionable. As a result, millions of consumer purchases could potentially be at risk.

In addition to contracts law in the US context, the IT manager should also be aware similar laws that exist in other countries, and the differences between these laws. Further, a new US law with a global reach as far as E-commerce is concerned is the Sarbanes-Oxley Act (2002), passed in response to a number of major corporate and accounting scandals involving prominent companies in the United States.

This topic will thus examine the extension of common-law contracts into cyberspace, the challenges that courts have confronted, and the application of new and pending state and federal legislation to address related challenges.

5. COURSE FORMAT

Class sessions

Ideally, this course will be jointly taught by two professors – one from the Information Systems department and one from the School of Law. The IS professor would ideally possess a background in IT strategy, IT and society, IT history, Security and Telecommunications and Networking. The law professor will ideally be skilled in Cyberlaw. This will ensure a balance between the technical aspects of IT and the legal issues pertaining to cyberspace. The class sessions will include classroom lectures interspersed with case discussions of some actual cases and rulings. The students will be challenged to actively participate by taking part in debates on constitutional issues. Guest lectures would include security experts, experts from the EFF and ACLU, policy makers and lawyers. The classroom lectures and discussions will be augmented by take home projects and assignments.

Projects and assignments

Assignments would include selected case studies on current court challenges. Students would also be required to develop "thought papers" commenting on any section of their syllabi. Group projects that would compare and contrast cyberlaws between the US and other countries would also be assigned.

6. CONCLUSION

In this paper we have argued that developments in IT necessitate that future IT managers need more than a cursory awareness of laws affecting IT, cyberspace and E-commerce. The current MSIS 2006 curriculum is beginning to recognize this need. However, no comprehensive course has emerged on Cyberlaw for IS managers. By contrast, cyberlaw is gaining acceptance as a full-fledged course in law schools in the US. We have borrowed some of the concepts and topics taught in a typical law school Cyberlaw course, and have adapted that to fit the graduate IS curriculum. We believe that this is a good start, and will help equip tomorrow's IT manager to deal with the appropriate tools to be cognizant of and effectively deal with cyberlaw issues in the IT environment.

7. REFERENCES

Burke, Lynne (2000). "Love Bug Case Dead in Manila," Wired Magazine, August 21, 2000. Retrieved on July 31, 2006 from http://www.wired.com/news/politics/0,1283,38342,00.html

Casey, E. (2004). *Digital Evidence and Computer Crime*. San Diego, CA. Elsevier.

Chon, Margaret (1999). "Introduction to Cyberspace." In *Learning Cyberlaw in Cyberspace.* Retrieved on July 31, 2006 from http://www.cyberspacelaw.org/modules.html#intro

Cybercrime (2006). *Wikipedia, The Free Encyclopedia*. Retrieved 14:28, April 3, 2006 from http://en.wikipedia.org/w/index.php?title=Cybercrime&oldid=46548752.

Easton, Eric (1999). "First Amendment in Cyberspace" In *Learning Cyberlaw in Cyberspace.* Retrieved on July 31, 2006 from http://www.cyberspacelaw.org/modules.html#first

Goldsmith, Jack and Tim Wu (2006). "Who controls the Internet? Illusions of a borderless world." Oxford University Press, 2006.

Gorgone, John T. and Paul Gray (1999). "MSIS 2000 Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems, Communications of the Association for Information Systems, (Volume 3, 2000)

Gorgone, John T., Paul Gray, Edward A. Stohr, Joseph S. Valacich and Rolf T. Wigand (2005). "MSIS2006 Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems." Communications of the Association for Information Systems (Volume 17, 2006), 1-56

Guidelines for Graduate Degree Programs in Information Systems, " Association for Computing Machinery (1999).

Kerr, Orin S. (2003) "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes." New York University Law Review, Vol 78, pp. 1596-1647, 2003

Lange, Maggie A. (2001) *Digital Music Distribution Technologies Challenge CopyrightLaw: A Review of* RIAA v. MP3.com *and* RIAA v. Napster, BOSTON B.J., Mar.–Apr. 2001.

Legislative Branch (2006, May 1). Federal government of the United States. In *Wikipedia, The Free Encyclopedia*. Retrieved 18:20, May 1, 2006 from http://en.wikipedia.org/w/index.php?title=Federal_government_of_the_United_States&oldid=50820243.

PC World Staff (1999). *The Digital Century: Software and the Internet.* Retrieved April 1, 2006 from http://www.cnn.com/TECH/computing/9911/23/digital.century2.idg/index.html

State, Tribe and local governments (2006, May 1). Federal government of the United States. In *Wikipedia, The Free Encyclopedia*. Retrieved 18:20, May 1, 2006 from http://en.wikipedia.org/w/index.php?title=Federal_government_of_the_United_States&oldid=50820243.

Symantec (2000). "'ILOVEYOU' Worm Wreaks Havoc Worldwide." Retrieved on July 31, 2006 from http://enterprisesecurity.symantec.com/article.cfm?articleid=97&PID=6526177

Legislations and Acts

Communications Decency Act. (2006, July 17). In *Wikipedia, The Free Encyclopedia*. Retrieved 20:16, July 31, 2006, from http://en.wikipedia.org/w/index.php?title=Communications_Decency_Act&oldid=64340847.

Computer Fraud and Abuse Act. (2006, April 23). In *Wikipedia, The Free Encyclopedia*. Retrieved 20:13, July 31, 2006, from http://en.wikipedia.org/w/index.php?title=Computer_Fraud_and_Abuse_Act&oldid=49695824.

Family Educational Rights and Privacy Act.1974. In *Wikipedia, The Free Encyclopedia*. Retrieved 19:06, July 31, 2006, from http://en.wikipedia.org/w/index.php?title=Family_Educational_Rights_and_Privacy_Act&oldid=63887207.

Health Insurance Portability and Accountability Act. 1996. In *Wikipedia, The Free Encyclopedia*. Retrieved 19:06, July 31, 2006, from http://en.wikipedia.org/w/index.php?title=Health_Insurance_Portability_and_Accountability_Act&oldid=66219756.

NET Act. (2006, July 25). In *Wikipedia, The Free Encyclopedia*. Retrieved 20:17, July 31, 2006, from http://en.wikipedia.org/w/index.php?title=NET_Act&oldid=65806228.

Privacy Act, 1974. Overview of the Privacy Act of 1974, US Department of Justice. http://www.usdoj.gov/04foia/04_7_1.html

Sarbanes-Oxley Act, 2002. In *Wikipedia, The Free Encyclopedia*. Retrieved 19:07, July 31, 2006, from http://en.wikipedia.org/w/index.php?title=Sarbanes-Oxley_Act&oldid=66219620.

USA PATRIOT Act. (2006, July 31). In *Wikipedia, The Free Encyclopedia*. Retrieved 18:48, July 31, 2006, from http://en.wikipedia.org/w/index.php?title=USA_PATRIOT_Act&oldid=66880659.

Cases cited

California v. Greenwood. (1987). US Supreme Court, Case number 86-684. Available online at http://laws.findlaw.com/us/486/35.html.

Playboy Enterprise Inc. v. Ferna. (1993). District Court, Florida, Case number 93-489-Civ-J-20.

US v. LaMacchia, 1994. Available online at http://www.loundy.com/CASES/US_v_LaMacchia.html