ISSN: 1545-679X

Information Systems Education Journal

Volume 8, Number 52 http://isedj.org/8/52/ July 16, 2010

In this issue:

An Exploration of the Legal and Regulatory Environment of Privacy and Security through Active Research, Guided Study, Blog Creation, and Discussion

Alan R. Peslak
Penn State University
Dunmore, PA 18512 USA

Abstract: One of the most important topics for today's information technology professional is the study of legal and regulatory issues as they relate to privacy and security of personal and business data and identification. This manuscript describes the topics and approach taken by the instructors that focuses on independent research of source documents and cases. Posting and review of this research with a blog served as a successful springboard for discussion and analysis of relevant privacy and security issues. The course was piloted in the spring of 2008 and received strong positive feedback. The course was successfully run again in 2009. Review of the process and implications for educators is presented.

Keywords: privacy, security, legal and regulatory environment of IT, ethics

---

Recommended Citation: Peslak (2010). An Exploration of the Legal and Regulatory Environment of Privacy and Security through Active Research, Guided Study, Blog Creation, and Discussion. *Information Systems Education Journal, 8* (52). http://isedj.org/8/52/. ISSN: 1545-679X. (A preliminary version appears in *The Proceedings of ISECON 2009:* §4352. ISSN: 1542-7382.)

This issue is on the Internet at **http://isedj.org/8/52/**

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)

This paper was in the 2009 cohort from which the top 45% were accepted for journal publication. Acceptance is competitive based on at least three double-blind peer reviews plus additional single-blind reviews by the review board and editors to assess final manuscript quality including the importance of what was said and the clarity of presentation.

An Exploration of the Legal and Regulatory Environment of Privacy and Security through Active Research, Guided Study, Blog Creation, and Discussion

Alan R. Peslak
arp14@psu.edu
Penn State University
Dunmore, Pennsylvania 18512 USA

Abstract

One of the most important topics for today's information technology professional is the study of legal and regulatory issues as they relate to privacy and security of personal and business data and identification. This manuscript describes the topics and approach taken by the instructors that focuses on independent research of source documents and cases. Posting and review of this research with a blog served as a successful springboard for discussion and analysis of relevant privacy and security issues. The course was piloted in the spring of 2008 and received strong positive feedback. The course was successfully run again in 2009. Review of the process and implications for educators is presented.

Keywords: Privacy, Security, Legal and Regulatory Environment of IT, Ethics

1. BACKGROUND

An area of rising importance for information technology professions is the growth of laws and regulations dealing with information and the use of information in society. This increased importance is mostly seen in rules and regulations regarding the privacy and security of data. But with this increased importance there has come little guidance on how to impart this knowledge to our information technology students.

One of the key templates for developing information systems and technology programs has been IS2002. IS 2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems is sponsored by the Association for Computing Machinery (ACM), Association for Information Systems (AIS), Association of Information Technology Professionals (AITP)and authored by John T. Gorgone, Gordon B. Davis, Joseph S. Valacich, Heikki Topi, David L. Feinstein, and Herbert E. Longenecker, Jr.

The legal, regulatory, privacy, and security related issues are suggested to be covered in the following courses general courses (they are a very small portion of each course):

IS 2002.1 – Fundamentals of Information Systems (Prerequisite: IS 2002.P0)

information security,

IS 2002.2 – Electronic Business Strategy, Architecture and Design (Prerequisite: IS 2002.1)

legal and ethical issues, information privacy and security, transborder data flows, information accuracy and error handling, disaster planning and recovery,

IS 2002.6 – Networks and Telecommunication (Prerequisite: IS 2002.4)

privacy, security,

IS 2002.P0 – Personal Productivity with IS Technology

security,

IS 2002.3 – Information Systems Theory and Practice (Prerequisite: IS 2002.1)

to introduce the societal implications of IS and related ethical issues

to introduce and explore ethical concepts and issues relating to personal and professional behavior

to introduce, compare, and contrast ethical models and approaches

to explore ethical and social analysis skills

to consider the nature and existence of power

ethical and legal principles and issues;

ethical considerations of information systems development, planning, implementation,

IS 2002.6 – Networks and Telecommunication (Prerequisite: IS 2002.4)

security, privacy,

IS 2002.2 – Electronic Business Strategy, Architecture and Design (Prerequisite: IS 2002.1)

security

Thus, the IS 2002 Model Curriculum included little emphasis on legal and regulatory aspects of IT. Contrasting this with the draft Computing Curricula 2005 shows how dramatically the need for legal and regulatory study has increased. The Computing Curricula 2005 includes five general computing curricula information technology, information systems, software engineering, computer engineering, and computer science. In all these five areas and with 17 computing topics as a part of these programs, legal/professional/ethics/society is recognized as one of the highest importance topics across all five areas, as high as programming fundamentals in a software engineering program and as high as computer architecture and organization in a computer engineering program. This topic is defined as: Legal / Professional / Ethics / Society – The areas of practice and study within the computing disciplines that help computing professionals make ethically informed decisions that are within the boundaries of relevant legal systems and professional codes of conduct.

To remedy this shortcoming a comprehensive three-credit course was developed at our university, IST 452 - Legal and Regulatory Environment of Privacy and Security (3) The short course description is, IST 452 Legal and Regulatory Environment of Privacy and Security (3) Exploration of legal, regulatory, public policy, and ethical issues related to security and privacy for information technology professionals in public institutions, private enterprise, and IT services. (Penn State University, 2008)

The course is further described in Appendix A.

The text used for the course the first time it was taught was e-Commerce Law: Issues for Business, 1st Edition , John W. Bagby - Pennsylvania State University, ISBN-10: 0324106793 ISBN-13: 9780324106794, 600 Pages. The text was used as a general guide for the course and also the source for some of the case analyses and discussion. Unfortunately this text is now out of print. We are searching for a new text.

The course was taught at our campus by a single instructor over two terms. The average size of the c;lass was 20 and all work was individual with major in-class discussion among all participants.

2. BLOG

One of the major elements of the course was the creation of a course blog. The syllabus included the following;

"The course will involve creation of a Blog that will serve as a comprehensive documentation of our semester long exploration. Participation will be frequent and required. Grading will be based on the general grading rubric. There will be six blogs in the course 3 each in the categories of course and case. Course or topic blog will be general definitions or specific research. Case will be thoughts and facts on specific IT law related cases." Thus, in addition to exploration of privacy and security topics, a second major blog was created to explore the review and opinions on case law relevant to privacy, security, and other IT law related topics. Many of these cases were found in the Bagby text but others were based on independent student research. Permission was received by students to include their materials in the article as examples.

3. LITERATURE REVIEW

There has been little pedagogical research on the content of the legal and regulatory environment of privacy and security. As well, there is little peer-reviewed pedagogical research done on privacy and security post-secondary education and most is focused solely on security issues. Hsu and Backhouse (2002) developed and proposed situated learning strategy to combine theory and practice in security education.

Kim, Hsu, and Stern (2006) performed a study of topics in the IS2002 curriculum with real world IT professionals and found that overall the individual most critical IS/IT issue was security and disaster recovery. Crowley (2003) suggests a comprehensive IT computer security curriculum that includes key knowledge and skills in "The current Information Systems Security regulatory and legal environment. Contemporary issues in computer security regulations and laws, including: Contract law Intellectual and other property law Criminal law Constitutional law Liability law Regulatory law. Principal ethical issues with relationship to legal standards. Distinguish the legal issues in an information architecture that can be analyzed by a computer security professional from those that require an attorney."

Kim and Surendran (2001) prepared a curriculum for information security manager that includes security requirements as well as security policy. Kroger and Sena (2002) prepared a comprehensive MBA course in "ethics, security, and privacy". The MBA course in ethics, security, and privacy suggested by Kroger and Sena (2002) starts with the Constitution and works through HIPAA as "the most significant example of an implementation of ethics, security, and privacy together." Other articles compare academic and government security standards (Carlin, Curl, and Manson, 2003), implementation of computer forensics in the classroom (2005), security issues associated with videocams (Beise, 2005), the inclusion of international components in security (2006), phishing (Frank and Werner, 2007), and mobile computing security in curriculum (Molluzzo and Lawler, 2007).

Overall, our course was designed to be an active, participatory course which explored all areas of IT privacy and security laws and regulations. The course relied on active research and class participation. The syllabus noted:

"This course will be unlike all other courses in IST. It will require significant critical thinking, problem solving, and written and oral communications. The course will involve creation of blogs that will serve as a comprehensive documentation of our semester long exploration. There will be significant required discussion to fully develop our critical thinking and communication skills."

This manuscript will define the major privacy and security areas covered in the course as well as inclusion of some of the annotated blog entries to both show the type of interaction which was generated as well as to serve as a general overview of the topic.

4. PRIVACY DEFINITION

The course began with an exploration and discussion of the term privacy in the information technology area. After a preliminary discussion of privacy and the Warren and Brandeis(1892) definition of privacy as the right to be left alone, as well as other common definitions, we started our first active research assignment. Our very first assignment was to search for a definition of privacy. Responses ranged from dictionary definitions to journals and vendor sites but overall the exploration and review of the blog provided a consensus on a starting point for our course. Example student response excerpts (in italics) will be shown for many of our major topics. Much more detail of these student responses is presented in Appendix B by topic. A responses for the privacy definition included:

"People often think of privacy as some kind of right. Unfortunately, the concept of a 'right' is a problematical way to start, because a right seems to be some kind of absolute standard. What's worse, it's very easy to get confused between legal rights, on the one hand, and natural or moral rights, on the other. It turns out to be much more useful to think about privacy as one kind of thing (among many kinds of things) that people like to have lots of. Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations. 4 demenstions of privacy: privacy of the person priva-

cy of personal behaviour privacy of personal communications privacy of personal data" - Roger Clarke http://www.anu.edu.au/people/Roger.Clarke /DV/Intro.html#Priv

5. PRIVACY AND MEDIA BASED ON WARREN AND BRANDEIS (1892) CONCEPTS

A specific assignment was to review Warrren and Brandeis privacy concepts in light of the current media environment. Each concept from the Warren and Brandeis was presented first and then discussed in light of present day media coverage.

1. The right to privacy does not prohibit any publication of matter which is of public or general interest. "Chris Brown hit a female in a club. Typically the newspapers protect the identity as they would any victim of domestic violence. The LA Times decided to run her name as the victim of the crime." http://www.feministing.com/archives/01363 4.html 2. The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel. "Defense Secretary Robert Gates ordered a review of a Pentagon policy banning media from taking pictures of flag-draped coffins of military dead, signaling he was open to overturning the policy to better honor fallen soldiers." http://www.google.com/hostednews/ap/artic le/ALeqM5iAudWAbfbRQ8W4w9LB2B9Bti__z QD968UAPG0 4. The right to privacy ceases upon the publication of the facts by the individual, or with his consent. Any person who publishes an autobiography.

After establishing the concept of privacy, we next explored the different types of laws. After a brief lecture, students were asked to find specific definitions and explanations of each type of law. Several students were assigned to each type of law and one answer is included below in *italics*.

6. TYPES OF LAW

Based on the Bagby text, the five general areas of law were explored: Criminal, Common, Procedural, Substantive, and Civil.

Substantive law defines how the facts in the case will be handled, as well as how the crime is to be charged. In essence, it deals with the "substance" of the matter. Substantive law refers to the body of rules that determine the rights and obligations of individuals and collective bodies. Source: http://criminal-law.freeadvice.com/criminal-law/procedural_substantive.htm and http://legal-dictionary.thefreedictionary .com/substantive+law

7. CONSTITUTION AND BILL OF RIGHTS

The cornerstone of privacy and security in the US is the Constitution and the first ten amendments known as the Bill of Rights. Many constitutional clauses and amendments were discussed including free speech, the commerce and contract clauses, and other articles. Some of the postings in this area are below.

IN 1971, PRESIDENT RICHARD M. NIXON'S ADMINISTRATION unsuccessfully tried to stop The New York Times from publishing a classified history of the Vietnam War known as the Pentagon Papers. In the process, the Supreme Court established that the First Amendment prohibits government censorship of the press in almost every situation. The First Amendment also protects press freedoms by making it exceptionally difficult for government officials and other public figures to win libel suits. (Libel is the publication of knowingly false statements that injure a person's reputation, the written form of slander.) If it were easy to sue for libel, the Supreme Court has reasoned, public figures could use lawsuits to keep the press from aggressively reporting the news. http://findarticles.com/p/articles/mi_m0BUE /is_3_139/ai_n17214796/pg_2?tag=artBody ;col1 Nixon tried to interfere with a NY times publication and was overruled by the supreme court. This was largely attributed to the rights the NY times has under the 1st amendment against government censorship.

The Commerce Clause of the Constitution gives the government - the power to regulate; that is, to prescribe the rule by which commerce is to be governed.

The Contract Clause of the Constitution – protects agreements whereby two parties bind themselves to certain obligations.

The First Amendment of the Constitution prohibits the United States from making laws infringing on free speech, religion, the press or restricting the right of a peaceful assembly or petition. One of the first cases we explored was Netscape vs. Specht which was illustrated in the Bagby text but also available in Wikipedia.org and along many other cases which can be found in http://itlaw.wikia.com

1. Key issues: - Are software license agreements binding or nonbinding? - User was not adequately notified of the agreement. 2. Decision For the agreement to be binding there must be mutual consent on behalf of both parties. 3. Alternatives First and foremost, Netscape could have charged for their service and, in charging, display to the user a more readily available end-user agreement which would not be as elusive as the previous agreement was.

Other cases included Reno v. Condon, Hiibel v. Sixth Judicial District Court of Nevada, and Hepting et al. v. AT & T Corp

8. COPYRIGHT, TRADEMARKS, PATENTS, TRADE SECRETS

The importance of understanding patents, copyrights, and trade secrets is reinforced by a current article in CIO magazine (Radcliffe and Rosen, 2003).

Copyright - form of protection provided by United States laws to original authors of original works of authorship (literary, dramatic, musical, artistic, and other intellectual works).

According to the government, trademarks include any word, name, symbol, or device, or any combination, used, or intended to be used in commerce to identify and distinguish the goods of one manufacturer or seller from goods manufactured or sold by others, and to indicate the source of the goods. Several students discussed specific trademark cases.

In addition, trade secrets and patents were discussed. According to the government, a patent for an invention is the grant of a property right to the inventor, issued by the United States Patent and Trademark Office. Generally, the term of a new patent is 20 years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. Trade secrets are not registered with the patent office and are internal secrets kept by a company. They have no specific protection but also no specific expiration.

9. THE DIGITAL MILLENNIUM COPYRIGHT ACT - DMCA

The Digital Millennium Copyright Act (DMCA) is a United States copyright law which implements two 1996 WIPO treaties. It criminalizes production and dissemination of technology, devices, or services that are used to circumvent measures that control access to copyrighted works (commonly known as DRM) and criminalizes the act of circumventing an access control, even when there is no infringement of copyright itself. It also heightens the penalties for copyright infringement on the Internet. (Wikipedia, 2008, DMCA) Several cases that explore the reach of DMCA were posted.

The RIAA subpoenaed Verizon demanding that Verizon reveal people who use or have used KazAa for music and file sharing. Verizon refused saying that the provision didn't cover possible copyright-infringing material that resides on individuals' own computers, only material that resides on an ISP's own computer. The courts agreed with Verizon and they were not required to give any information regarding people who used Peer to Peer filesharing software. Sources: http://www.eff.org/related/376/case

10. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT - HIPAA

Breaux and Anton (2008) provide a framework for "analyzing regulatory rules for privacy and security" and use HIPAA (US Health Insurance Portability and Accountability Act) as an example, breaking down the act into specific components and requirements. They note that HIPAA is one of the most important laws regarding privacy as the" 10-year cost to comply with HIPAA for the healthcare industry is projected by industry and government stakeholders to be between $12-42 billion". There are two general rules associated with HIPAA – privacy and security. Privacy Rule – established minimum federal standards for protecting the

privacy of individually identifiable health information. Security Rule – measures a healthcare entity must take to protect personal health information from unauthorized breaches of privacy. Example postings include:

In July of 2008, a Seattle health provider was fined $100,000 and forced to create a corrective action plan after losing backup media and laptops containing records from 2005 and 2006. The items lost include backup tapes, optical discs, and unencrypted laptops. The information contained on the devices is personally identifiable and could have affected more than 360,000 patients. As a corrective action, the health provider must train employees how to safeguard information and the facilities. According to the article, it appears that the government was stepping up enforcement as the agency could resolve problems last year rather than punish mistakes. *http://itknowledgeexchange.techtarget.com/security-bytes/hipaa-violations-cost-seattle-health-care-provider/*

11. PATRIOT ACT

Regarding the PATRIOT Act, "Mark Corallo, a Justice Department spokesman, …said the act has been "one of the most important tools Congress has given the government to fight terrorism and prevent terrorist acts." It is also one of the most important laws affecting privacy and security in the United States.(Garcia, 2004)

A detailed review of the PATRIOT act was included in our course. The major provisions or "titles" are as follows: Titles I and X: Miscellaneous Provisions, Title II: Surveillance Procedures, Title III: Anti-money-laundering to Prevent Terrorism, Title IV: Border Security, Title V: Terrorism Investigation, Title VI: Victims and Families of Victims of Terrorism, Title VII: Information Sharing for Infrastructure Protection,, Title VIII: Terrorism Criminal Law, Title IX: Improved Intelligence. Our assignment was to look at current developments in PATRIOT act interpretation.

A ruling in 2007 in U.S. District Court says that agencies such as the FBI can no longer request that Internet and telephone companies turn over the records of the customers without telling them and without eventually obtaining a court order. In short, this means that the agencies must show purpose for their seizure of records, whereas before their national security letters had protected them from basically almost any accountability. This ruling is important because it takes away the capabilities of the government to seize data without probable cause, thus further upholding the principles of the constitution.
http://articles.latimes.com/2007/sep/07/nation/na-patriot7

12. SURVEILLANCE/ANTI-TERRORISM IN OTHER NATIONS

Surveillance and Anti-terrorism laws and regulations in many other nations were explored. An example was New Zealand.

The interception of telecommunication is governed by many laws in New Zealand including the Telecommunications Act, Government Communications Security Bureau Act, ,International Terrorism Act, Misuse of Drugs Amendment Act, New Zealand Security Intelligence Service Act, and Crimes Act.

13. INTERNET SAFETY ACT

A new proposed act, the Internet Safety Act was explored in 2009.

The Internet Safety Act is aimed at everyone. Its purpose is to have data just in-case someone breaks a law. The law would reach everyone from the giant corporate ISPs right down to a single private citizen who has a password protected access point. Unlike phone carriers, they would have be required to store usage data for an extended amount of time.
http://www.networkworld.com/news/2009/022109-proposed-law-might-make-wi-fi.html?page=2

14. FTC, PRIVACY POLICIES AND FAIR INFORMATION PRACTICE GUIDELINES

Fair Information Practices as promulgated by the FTC play an important role in online privacy.

"Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information -- their "information practices" -- and the

safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices. Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress." (FTC, 2000) Students reviewed the policies and were asked to write sample company privacy policies.

15. UNITED STATES VS. EUROPEAN FAIR INFORMATION AND PRACTICES

The differences between the United States Fair Information Practices and those of the European Union were extensively discussed. Country implementations of the directive were explored.

With the European Union Directive 95/46 setting guidelines for maintaining privacy for user data, Germany passed its own law in 2002 called the Data Protection Act. This act defines what constitutes data collection and processing, consent of the user whose data is being collected, acceptable transfer of the collected data, and the responsibilities of the individual, group, business, etc. that is collecting the data regarding maintaining adequate security. It also outlines the creation and maintenance of a security official who is held responsible for maintaining the data collected. This act is much more thorough than the EU Directive. http://www.bdd.de/Download/bdsg_eng.pdf

16. SAFE HARBOR ACT FRAMEWORK

The following areas were explored in the Safe Harbor Act seven privacy principles, 15 frequently asked questions and answers (FAQs), the European Commission's adequacy decision, the exchange of letters between the Department and the European Commission, and letters from the Department of Transportation and FTC on their enforcement powers.

The European Commission's Directive on Data Protection went into effect in October, 1998, and would prohibit the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin. As a result of these different privacy approaches, the Directive could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" framework. The safe harbor -- approved by the EU in 2000-- is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the safe harbor will assure that EU organizations know that your company provides "adequate" privacy protection, as defined by the Directive. (Department of Commerce, n.d.)

17. SARBANES OXLEY ACT

The Sarbanes Oxley Act which established new or enhanced standards for all U.S. public company boards, management, and public accounting firms in the aftermath of Enron and Worldcom scandals was also included in our course.

Why didn't Sarbanes-Oxley prevent the subprime mortgage crisis? That is the unspoken question asked in a piece titled "Criminalizing Capitalism" written by a Manhattan Institute scholar, Nicole Gelinas. She reminds us that the legislation passed in the wake of the Enron scandal was meant to reform corporate governance and head off punishing meltdowns of investor wealth. It hasn't. Instead, what Sarbox did was to open the door

to excessive and sometimes careless criminal prosecution of corporate wrongdoing. The savaging of AIG and of the now-defunct Arthur Anderson are cases in point. According to Ms. Gelinas, the 20-year prison sentences available to prosecutors has created an environment of fear in the executive suite, which in turn has led to a wanton disregard for the rights of corporate defendants and, on occasion, flagrantly unfair treatment of companies and individuals. http://www.nysun.com/business/why-sarbanes-oxley-didnt-prevent-the-latest-crisis/71321/

18. UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT - UCITA

Students were asked to discuss pros and cons of the Uniform Computer Information Transactions Act, a proposed law to create a clear and uniform set of rules to govern such areas as software licensing, online access, and other transactions in computer information.

http://www.aaxnet.com/topics/ucita.html
This website basically breaks down each part of this act that is being proposed. Some of the most interesting things about this that I found, and some of the more unsettling parts of it, were that if it were passed, you would be prohibited from selling a PC with any software on it. If you were selling a windows-based PC, you would have to unistall the operating system before you sold it, otherwise it would be illegal. Another interesting part of it is that it would make it illegal to talk smack about any piece of software from any manufacturer. For instance, if you had a piece of software installed on your system and it didn't work, and you could prove it didn't work, and you talked smack about it, you could be sued by the company that manufactured that piece of software (a sort of slander similarity). I think this act is bad news all around and should not be passed. I can't believe that it would even uphold any challenges to it.

19. CAN-SPAM

The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them. (FTC, n.d.). One of our exercises was to argue pro and con on the CAN-SPAM act.

20. FAIR USE

Under limited circumstances a copyrighted work can be used by another. This is called fair use and was a week's topic. Included in the cases were Field v. Google Inc, Campbell v. Acuff-Rose Music, Eloise Toby Marcus v Shirley Rowley and San Diego Unfiled School District, Grand Upright Music, Ltd. v. Warner Bros. Records, Inc., Castle Rock Entertainment, Inc. v. Carol Publishing Group, Inc , Basic Books, Inc. v. Kinko's Graphics, Rogers v. Koons, Harper & Row v. Nation Enterprises, Higgins v. Detroit Educational Television Foundation. Fair use was extensively discussed including the Obama Hope poster.

21. FAIR CREDIT REPORTING ACT - FCRA

"The Fair Credit Reporting Act (FCRA) is a federal law that regulates how credit reporting agencies use your information. Enacted in 1970 and substantially amended in the late 1990s and again in 2003, the FCRA restricts who has access to your sensitive credit information and how that information can be used." (Equifax, 2007) http://www.equifax.com/cs/Satellite?pagename=elearning_credit14

Cases included Killingsworth v. HSBC Bank Nevada, Maria et al v. Apple Computer, Inc, Heather Gillespie and Angela Cinson v. Equifax Information Services, L.L.C. and Experian vs. LifeLock Lawsuit.

Again, permission was received by students to include their materials in the article as examples.

22. CONCLUSION

The result of the course was very favorable. The active research approach and use of Web 2.0 tools especially blogs has been met with enthusiasm in our class this past semester. This is a typical response to the overall course survey. *"Overall this was a very interesting and informative class. The topics*

we covered are all issues that at some point in our professional careers we will encounter. This class will prepare us to better deal with issues we encounter regarding legalities, or at least lend us the resources to be able to find ways to better deal with these issues."

23. REFERENCES

Beise, C M. "Global Media: Incorporating Videocams and Blogs in a Global IS Management Class. " In The Proceedings of ISECON 2005, v 22 (Columbus OH): §2143. ISSN: 1542-7382.

Breaux, T. and Anton, A. (2008) "Analyzing Regulatory Rules for Privacy and Security Requirements" IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 34, NO. 1, JANUARY/FEBRUARY 2008 p.5-20

Carlin, A, S S Curl, and D P Manson. "To Catch a Thief: Computer Forensics in the Classroom" In The Proceedings of ISECON 2005, v 22 (Columbus OH): §3574. ISSN: 1542-7382.

Chepaitis, E V. "Information Systems Archeology and Other Experiential Projects: Toward Broader Information Literacy Education." In The Proceedings of ISECON 2003, v 20 (San Diego): §3222. ISSN: 1542-7382. (Revised and expanded version appears in Information Systems Education Journal 2(20). ISSN: 1545-679X.)

Crowley, E. (2003) "Information system security curricula development" CITC4 '03: Proceedings of the 4th conference on Information technology curriculum 249-255.

Equifax (2007) http://www.equifax.com/cs/Satellite?pagename=elearning_credit14

Equifax (2007) "Your Credit RightsKey Rights Contained in the Fair Credit Reporting Act (FCRA)" http://www.equifax.com/cs/Satellite/EFX_Content_C1/1165255680510/5-1/5-1_Layout.htm

Fair Information Practice Principles FTC (2007) http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Forster, W P and T Tam. "Weblogs and Student-Centered Learning: Personal Experiences in MBA Teaching." In The Proceedings of ISECON 2004, v 21 (Newport): §3242. ISSN: 1542-738

Frank, C E and L A Werner. "Getting A Hook On Phishing." In The Proceedings of ISECON 2007, v 24 (Pittsburgh): §3523. ISSN: 1542-7382. (Revised in Information Systems Education Journal 5(36). ISSN: 1545-679X.)

FTC (2007). "Privacy Online." http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

FTC n.d. "The CAN-SPAM Act: Requirements for Commercial Emailers" http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.shtm

Garcia, M. (2004) N.Y. "City Council Passes Anti-Patriot Act Measure," The Washington Post Thursday, February 5, 2004; Page A11

Gorgone, J., Davis, G., Valacich, Topi, H., Feinstein, D. and Longenecker, H. (2002) "IS 2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems is sponsored by the Association for Computing Machinery (ACM), Association for Information Systems (AIS), Association of Information Technology Professionals."

Hsu C. and Backhouse, J. (2002) "Information systems security education: Redressing the balance of theory and practice." Journal of Information Systems Education; 2002; 13, 3 p.211-218.

Joint Task Force for Computing Curricula 2005 (2006) "Computing Curricula 2005 The Overview Report covering undergraduate degree programs in Computer Engineering Computer Science Information Systems Information Technology Software Engineering A volume of the Computing Curricula Series" Page ii

Kim, K Y and K Surendran. "A Curriculum Development For Information Security Manager Using DACUM." In The Proceedings of ISECON 2001, v 18 (Cincinnati): §39a.

Kim, Y. Hsu, J., Stern, M. (2006) "An Update on the IS/IT Skills Gap." Journal of Information Systems Education; Winter 2006; 17, 4; 395-402.

Kroger, D J and M P Sena. "An MBA Course in Ethics, Security, and Privacy." In The Proceedings of ISECON 2002, v 19 (San Antonio): §254a. ISSN: 1542-7382.

Manson, D P and S S Curl. "A Comparison of Academic and Government Information Security Curriculum Standards." In The Proceedings of ISECON 2003, v 20 (San Diego): §2241. ISSN: 1542-7382. (Revised in Information Systems Education Journal 1(39). ISSN: 1545-679X.)

Marchant, R L, R Cole, and C H Chu. "Answering the Need for Information Assurance Graduates: A Case Study of Pennsylvania State University's Security and Risk Analysis Major". In The Proceedings of ISECON 2007, v 24 (Pittsburgh): §3345. ISSN: 1542-7382.

Molluzzo, J C and J P Lawler. " Integrating Issues of Location-based Privacy with Mobile Computing into International Information Systems Curricula." In The Proceedings of ISECON 2007, v 24 (Pittsburgh)

Penn State University (2008) "IST 452 Course Description" http://bulletins.psu.edu/bulletins/bluebook/university_course_descriptions.cfm?letter=I&courselong=ist|452|latest

Radcliffe, M. and Rosen, L. (2003) "Patent, Copyright and Trade Secret--What's the Difference?" CIO http://www.cio.com/article/29593/Patent_Copyright_and_Trade_Secret_What_s_the_Difference_

Safe Harbor, US Department of Commerce n.d. http://www.export.gov/safeharbor/sh_overview.html

White, G L and J Long.(2006) "Thinking Globally: Incorporating an International Component in Information Security Curriculums." In The Proceedings of ISECON 2006, v 23 (Dallas): §2324. ISSN: 1542-7382. (Revised in Information Systems Education Journal 5(39). ISSN: 1545-679X.)

Wikipedia (2008) "Communications Decency Act " http://en.wikipedia.org/wiki/Communications_Decency_Act

Wikipedia (2008) "DMCA" http://en.wikipedia.org/wiki/DMCA

APPENDIX A

Full Course Description

"IST 452 Legal and Regulatory Environment of Privacy and Security (3) Institutional constraints on security historically focused on traditional criminal enforcement and a slow but steady increase in civil remedies through the twentieth century. Professional security protection could satisfy reasonable assurance criteria by managing legal and regulatory risks based on commonly-held understandings of burglary, theft, conversion and widely-understood but related institutional constraints in the protection of physical property. This focus retained effectiveness so long as physical security over tangible property appeared successful, even extending to the maintenance of control over mainframe computers and their peripherals. However, the proliferation of networked computers has made access and storage ubiquitous, vastly increasing the vulnerability of confidential data, private information and critical national security infrastructure. Security and privacy regulation compliance responsibility now falls much more harshly on both organizations and most of their individual personnel. These complex new duties constrain organizations in the data management industry as well as suppliers and users of data and all participants in the information supply chain, including consultants, software suppliers, applications service providers, maintenance, outsourcing and communications providers.

Other factors exacerbate these liability risk management difficulties. Advances in network computer storage and use, the broadening perception of heightened value of information and the pervasive availability of rich data warehousing increase the vulnerability of data management. Risks of information theft and integrity losses as well as the explosion of privacy rights and national security concerns now require pervasive and fuller understanding of liability risk management principles/techniques among all managers and subordinates in the data management industry and in government. Information suppliers, handlers, owners and network service providers are increasingly exposed to civil litigation, regulatory oversight/compliance and criminal prosecution for various information-related wrongs. For example, confidentiality is compulsory for corporate trade secrets, privacy is required for personally identifiable information about individuals and secrecy is mandatory over matters of national security; all of which create complex legal duties that are fundamentally driving the design of information handling processes. This course surveys legal and regulatory constraints on information security and privacy practices." (Penn State University, 2008)

APPENDIX B

Further Student Responses

Privacy definition

Privacy Definition In general, the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed. In specific, privacy may be divided into four categories (1) Physical: restriction on others to experience a person or situation through one or more of the human senses; (2) Informational: restriction on searching for or revealing facts that are unknown or unknowable to others; (3) Decisional: restriction on interfering in decisions that are exclusive to an entity; (4) Dispositional: restriction on attempts to know an individual's state of mind. http://www.businessdictionary.com/definition/privacy.html

I found a couple of different ones that I like: In the 1890s, future United States Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's "right to be left alone." Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should be reflected in the Constitution Robert Ellis Smith, editor of the Privacy Journal, defined privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves." According to Edward Bloustein, privacy is an interest of the human personality. It protects the inviolate personality, the individual's independence, dignity and integrity. According to Ruth Gavison, there are three elements in privacy: secrecy, anonymity and solitude. It is a state which can be lost, whether through the choice of the person in that state or through the action of another person. The Calcutt Committee in the United Kingdom said that, "nowhere have we found a wholly satisfactory statutory definition of privacy." But the committee was satisfied that it would be possible to define it legally and adopted this definition in its first report on privacy: The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information. The Preamble to the Australian Privacy Charter provides that, "A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy...Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech...Privacy is a basic human right and the reasonable expectation of every person." Aspects of Privacy Privacy can be divided into the following separate but related concepts: Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection"; Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches; Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks. Source http://www.privacyinternational.org/survey/phr2003/overview.htm

Privacy and media based on Warren and Brandeis (1892) concepts

1. Example of right to privacy does not prohibit publication of what is considered to be of public or general interest: Casey Anthony, charged with her daughter's murder, has had all of her visits with family members through a jail telephone videotaped and then released to the media. 2. Example of right to confidential information: Presidents are required to release their health records to the public and must reasonably notify the public of such events (such as if a President is going to be incapacitated because of a colonoscopy) the nation is notified that the Vice President will briefly assume duties. 3. Privacy with content example: When you are admitted to a hospital, in accordance with HIPAA, they ask if someone calls the hospital and asks

if you are here or for your room number if the hospital could confirm this to the person who called. If you say yes, they can let others know, you have waived this right to privacy.

1. Libel and Slander Stemming from a case in which an elected official in Montgomery, Ala., complained of defamation by civil-rights activists, the court ruled that to protect the free flow of speech and opinions, public officials could only collect damages for libel if falsehoods were made with "reckless disregard" for the truth.

Types of Law

Based on the Bagby text, the five general areas of law were explored: Criminal, Common, Procedural, Substantive, and Civil.

Procedural law is law describing how substantive law is enforced by entailing the formal steps which must be taken to enforce legal rights. This includes things like jurisdiction, jury selection, counsel, as well as post-trial aspects such as appeals and enforcement of punishments. http://law.jrank.org/pages/9455/Procedural-Law.html
http://www.answers.com/topic/procedural-law

http://topics.law.cornell.edu/wex/Criminal_law criminal law: an overview Criminal law involves prosecution by the government of a person for an act that has been classified as a crime. Civil cases, on the other hand, involve individuals and organizations seeking to resolve legal disputes. In a criminal case, the state, through a prosecutor, initiates the suit, while in a civil case the victim brings the suit. Persons convicted of a crime may be incarcerated, fined, or both. However, persons found liable in a civil case may only have to give up property or pay money, but are not incarcerated.

Common law A system of law that is derived from judges' decisions (which arise from the judicial branch of government), rather than statutes or constitutions (which are derived from the legislative branch of government). http://www.ll.georgetown.edu/tutorials/definitions/common_law.html The common law is more malleable than statutory law. First, common law courts are not absolutely bound by precedent, but can (when extraordinarily good reason is shown) reinterpret and revise the law, without legislative intervention, to adapt to new trends in political, legal and social philosophy. Second, the common law evolves through a series of gradual steps, that gradually works out all the details, so that over a decade or more, the law can change substantially but without a sharp break, thereby reducing disruptive effects. In contrast, the legislative process is very difficult to get started, and legislatures tend to delay acting until a situation is totally intolerable. For these reasons, legislative changes tend to be large, jarring and disruptive (either positively or negatively). http://en.wikipedia.org/wiki/Common_law

Constitution and Bill of Rights

The Commerce Clause of the Constitution gives the government - the power to regulate; that is, to prescribe the rule by which commerce is to be governed.

Wabash, St. Louis & Pacific Railway Co. v. Illinois Citation: 118 U.S. 557 (1886) Concepts: Individual Property Rights v. State Rights/Commerce Clause Facts An Illinois statute imposed a penalty on railroads that charged the same or more money for passengers or freight shipped for shorter distances than for longer distances. The railroad in this case charged more for goods shipped from Gilman, Illinois, to New York, than from Peoria, Illinois, to New York, when Gilman was eighty-six miles closer to New York than Peoria. The intent of the statute was to avoid discrimination against small towns not served by competing railroad lines and was applied to the intrastate (within one state) portion of an interstate (two or more states) journey. Issue Whether a state government has the power to regulate railroad prices on that portion of an interstate journey that lies within its borders. Opinion The Supreme Court of the United States held the Illinois statute to be invalid and that the power to regulate interstate railroad rates is a federal power which belongs exclusively to Congress and, therefore, cannot be exercised by individual states. The Court said the right of continuous transportation from one end of the country to the other is essential and that states should not be permitted to impose restraints on the freedom of commerce. In this decision, the Court gave great strength to the

commerce clause of the Constitution by saying that states cannot impose regulations concerning price, compensation, taxation, or any other restrictive regulation interfering or seriously affecting interstate commerce. http://www.tourolaw.edu/patch/casesummary.asp

The Contract Clause of the Constitution – protects agreements whereby two parties bind themselves to certain obligations.

Peevyhouse v. Garland Coal & Mining Co., (1962) 2. Facts: Peevyhouse leased part of their farm to Garland Mining for strip mining of coal. The express written contract stated that one of the terms of the contract was that Garland smooth out the land once it was done strip mining. After all the mining was done, Garland refused to smooth out the land, and Peevyhouse sued for the cost of completion of moving the dirt back, which was estimated at $29,000. However, Peevyhouse's farm was only worth less than $5,000, and the increase in value of the farm would only be $300 if the dirt were to be smoothed out. The trial jury returned a verdict of $5,000 which did not match either party's theory of damages. 3. Nature of the Risk: The farmer risked that he could make more money if he leased his farm to someone else. The miner risked that he could make more money if he leased a different farm for strip mining. 4. Issue: Is the proper measure of damages the cost of completing the terms of the contract, even though they outweigh the value of performance significantly? 5. Holding: No. Where the cost of completion of a contract is disproportionate to the "end to be attained" the proper measure of damages is the difference in value if the contract were fully performed. 6. Reasoning: The majority reasoned that the farmer would unlikely be willing to pay $29,000 to make improvements to his property that would increase its value only $300. So to award him the $29,000 would be a windfall. Thus, the primary purpose of the contract was to recover coal from the ground to the benefit of both parties, not to regrade the land. http://www.lectlaw.com/files/lws49.htm

The Digital Millennium Copyright Act

Summary:Three software programmers who created the BNETD game server (using an open source program), which allowed users to play Blizzard games online with other gamers without the use of Blizzard's Battle.net service, were accused of being in violation of of the DMCA and Blizzards EULA by circumventing the software to allow the play on non-Blizzard servers. The programmers argued that they should be allowed to create free software to allow people to use commercial products because it was beneficial to the consumer and spawned innovation. It was ruled, however, that the reverse engineering and emulation of Blizzards's software was illegal and in violation of the DMCA. http://www.eff.org/cases/blizzard-v-bnetd

Health Insurance Portability and Accountability Act

Basically CVS got lazy and just threw away their patients empty bottles in the regular garbage can so anyone could have access to it and now they are paying for it. They said that the employees weren't properly trained on how to dispose of them. Here's the facts: CVS will pay the government $2.5 million and toughen their practices so that the privacy of patients is not violated. The settlement which applies to all CVS retail pharmacies is in response to the HHS Office of Civil Rights (OCR) and their extensive investigation concerning HIPAA violations. In a coordinated action, CVS also signed a consent order with the FTC to settle potential violations of the FTC Act. OCR opened an investigation in response to media reports that alleged that patient information maintained by the pharmacy chain was being disposed of in industrial trash containers outside selected stores and were not secure and could be accessed by the public. According to the information, CVS also failed to adequately train employees on how to dispose of such information properly. At the same time, FTC also opened an investigation of CVS and this resulted in both agencies working to coordinate the investigation. Under the HHS resolution agreement, CVS agreed to pay the $2.25 million and implement a robust corrective action plan. CVS will also actively monitor its compliance and the FTC consent order. The monitoring requirement specifies that CVS must engage a qualified independent third party to assess CVS compliance and then submit reports to the federal agencies. The HHS corrective action plan will be in place for three years while the FTC plan will be monitored for 20 years. Source: http://telemedicinenews.blogspot.com/2009/02/hipaa-case-settled.html

Patriot Act

Summary: In Sept of 2004, a federal judge in New York ruled that the component of the PATRIOT Act which allows the FBI to demand information from ISP's is unconstitutional as it does not allow for judicial oversight or public review. The case was originally filed by the ACLU on behalf of an unnamed ISP which challenged a NSL which demanded the information. The judge ordered the Justice Dept to halt the use of NSL's, however he provided a 90 injunction to allow for an appeal. Since NSL's are still in use...my guess is the Government won the appeal. http://www.washingtonpost.com/wp-dyn/articles/A59626-2004Sep29.html

A man and his daughter were looking at stars and temporarily blinded the pilot and co-pilot of an airplane with a laser beam for the telescope. Authorities used the Patriot Act to charge the man with interfering with the operator of a mass transportation vehicle and making false statements to the FBI. He was the first person arrested after a recent rash of reports around the nation of laser beams hitting airplanes. Source: ttp://www.foxnews.com/story/0,2933,143371,00.html September 7, 2007

NEW YORK - A federal court today struck down the amended Patriot Act's National Security Letter (NSL) provision. The law has permitted the FBI to issue NSLs demanding private information about people within the United States without court approval, and to gag those who receive NSLs from discussing them. The court found that the gag power was unconstitutional and that because the statute prevented courts from engaging in meaningful judicial review of gags, it violated the First Amendment and the principle of separation of powers.] http://www.aclu-mn.org/home/news/courtstrikesnationalsecuri.htm This article goes on to tell that in the case Doe v. Gonzales which was originally filed in 2004 on behalf of an anonymous Internet access company a National Security Letter was received. The presiding judge, Marrero struck down the gag orders issued by the government to the website stating that the Gag was unconstitutional. The article reviews several other interesting cases regarding this. Very good read!

Surveillance/Anti-terrorism in other nations

Spain - Secret military telecommunications interception stations in Madrid, Conil de la Frontera, Gibraltar and Rota [It is significant that the station is run by the military. The former Spanish intelligence agency (CESID) was run by the military, and was recently replaced by a civilian agency, the CNI (National Intelligence Centre, see Statewatch vol 11 no 3 & 4). This change was partly motivated by a lack of accountability, and of a clear legal basis for interception, that resulted in the illegal interception of Spanish citizens in the past. The CNI is subject to interception guidelines requiring a judicial warrant for the interception of communications involving Spanish citizens, which are protected from interference by the Spanish constitution, although telephone tapping was not regulated until the new law was passed last year.]

http://www.statewatch.org/news/2004/aug/10spain-gib-comint.htm

In 1975 Telecommunication tactics were taken by the Spanish government, though they were kept secret and there was no law governing them. The CESID or Spanish Intelligence Agency was monitoring telecommunication lines of Spanish citizens. Spanish citizens are protected from this interference under their constitution. Santiago programme has taken over for the CESID as of 2008 and are now in charge of these internal affairs.

I guess before this law was passed it was illegal for any agency to use wiretapping in Japan. It was passed in 1999 but was enacted in 2000 because of the massive amount of amendments. "The law permits the law enforcement agencies (LEAs) to intercept communications on phone, fax, and the Internet in criminal cases involving organized murder, illicit firearms trade, drug trafficking, and smuggling of illegal immigrants into Japan. However, the communications of doctors, lawyers, and religious leaders cannot be intercepted under the law and media communications can only be intercepted under certain conditions. The law also directs ISPs to maintain a log of all the Internet communications that are monitored at any time." Only Police officers that are superintendent and above can execute wiretapping upon receipt of an authorized warrant. The law also requires the presence of a third-party non-police witness, such as

an employee of either the communication service provider or regional government, for monitoring the wiretapping process. In addition, LEAs are required to notify individuals (whose communications have been intercepted) within 30 days of concluding the investigation and all documents pertaining to the communication must be destroyed thereafter. The law does not define the devices or surveillance tools that can be used for lawful interception

Internet Safety Act

This act states that it will require all Internet providers and operators of millions of Wi-Fi access points, even hotels, local coffee shops, and home users, to keep records about users for two years to aid police investigations. I think that this would be ideal for all business but to bring it into a home I think would violates someones privacy. One thing that I wonder is who and where would this be stored and who would be responsible for keeping it. My grandfather wouldn't be able to do this and he has a WLAN set up in his house. Source: http://news.cnet.com/8301-13578_3-10168704-38.html

An incredibly interesting feature of the Internet Safety Act is the current proposed wording in terms of keeping logs to help prevent child pornography. While it is probably a good (but questionable) idea for the ISPs to keep logs of what users access, it will also require all providers of access points to keep logs of user activity. This is excessive because many users of wifi, especially home users like myself, is pretty much beyond the realm of understanding of most end users. Overall, I know that an act like this could help kids be safer online, but the most effective method would be for parents to start doing their jobs. Either way, I would consider myself an advanced user and I don't see how even people on my level could effectively keep logs. Also, what if back up systems fail? That happens all the time! http://www.thetechherald.com/article.php/200908/2998/Opinion-Internet-SAFETY-Act-%E2%80%93-you-ll-need-to-keep-your-logs-or-go-to-jail

United States vs. European Fair Information and Practices

With the European Union Directive 95/46 setting guidelines for maintaining privacy for user data, Germany passed its own law in 2002 called the Data Protection Act. This act defines what constitutes data collection and processing, consent of the user whose data is being collected, acceptable transfer of the collected data, and the responsibilities of the individual, group, business, etc. that is collecting the data regarding maintaining adequate security. It also outlines the creation and maintenance of a security official who is held responsible for maintaining the data collected. This act is much more thorough than the EU Directive. http://www.bdd.de/Download/bdsg_eng.pdf

Sarbanes Oxley Act

FEI Survey: Average 2007 SOX Compliance Cost $1.7 Million

-Audit Fees Show Slight Increase to $3.6 Million-

-More Companies See Benefit, Note Positive Changes to Audit-

http://fei.mediaroom.com/index.php?s=43&item=204

Uniform Computer Information Transactions Act - UCITA

The UCITA was originally proposed as an amendment to the UCC Act. It governs the sale of software, databases and other relevant contracts involving information. One thing that it accomplishes is that it standardizes laws relating to information across states, which many other bills fail to do. The act has, however, faced a significant amount of opposition, as many feel that it was written on the coat tails of software lobbyists rather than in the best interests of the people. The act does, ultimately, get ridiculous, as it gives benefits to businesses over consumers. For example, as I read, if I buy a video game and finish it, I should not be able to sell it to my friend according to UCITA. It also lessens the accountability of software companies (Windows Vista anyone?. http://www.badsoftware.com/uccindex.htm http://www.badsoftware.com/uccindex.htm#Background

Fair Use

Summary: Kinkos was found to be in violation of copyright laws when photocopied sections of school books were sold to students as "coursepacks" for their university classes. Three of the four requirements of fair use were met, however the impact on the market was what led the court to rule against Kinkos. It was believed that by including these copies in a "coursepack" the original publishers of the books would lose a significant amount of revenue since the entire book was not being purchased. COPYING FOR EDUCATION Basic Books, Inc. v. Kinko's Graphics Corp.,758 F.Supp. 1522 (S.D.N.Y. 1991). Kinko's was held to be infringing copyrights when it photocopied book chapters for sale to students as "coursepacks" for their university classes. Purpose: When conducted by Kinko's, the copying was for commercial purposes, and not for educational purposes. Nature: Most of the works were factual-history, sociology, and other fields of study-a factor which weighed in favor of fair use. Amount: The court analyzed the percentage of each work, finding that five to twenty-five percent of the original full book was excessive. Effect: The court found a direct effect on the market for the books, because the coursepacks competed directly with the potential sales of the original books as assigned reading for the students. Conclusion: Three of the four factors leaned against fair use. The court specifically refused to rule that all coursepacks are infringements, requiring instead that each item in the "anthology" be subject individually to fair-use scrutiny. http://www.copyright.iupui.edu/FUsummaries.htm Entire details: http://www.bc.edu/bc_org/avp/cas/comm/free_speech/basicbooks.html

Again, permission was received by students to include their materials in the article as examples.

APPENDIX C – PARTIAL SYLLABUS

IST 452 - Legal and Regulatory Environment of Privacy and Security (3)

Credit Hours: 3.0

Official Course Description:

IST 452 - Legal and Regulatory Environment of Privacy and Security (3) Exploration of legal, regulatory, public policy, and ethical issues related to security and privacy for information technology professionals in public institutions, private enterprise, and IT services.

Prerequisite: IST 301 or SRA 231 or equivalent

Course Objectives:

Upon completion of the course, the student will be able:

To understand common legal, ethical, and regulatory issues associated with Information Technology as it relates to both security and privacy.

In addition the student will understand:

Common legal terms related to e-commerce

Current US and major international laws and regulations regarding privacy and security

Specific exploration, interpretation, and understand will include:

Privacy Polices

HIPPA

PATRIOT act

UCC

Sarbanes-Oxley

UCITA

Contracts

Copyrights

Patents

Fair Information Practices

Background for the course

This course will be unlike all other courses in IST. It will require significant critical thinking, problem solving, and written and oral communications. The course will involve creation of Blogs that will serve as a comprehensive documentation of our semester long exploration.

There will be significant required discussion to fully develop our critical thinking and communication skills.

Required Texts:
Privacy, Information and Technology Second Edition by Daniel J. Solove (Author), Paul M. Schwartz (Author) (2009)
Aspen Publishers
ISBN-13: 978-0735579101

Additional online content.

Significant resources will be posted in ANGEL.

Required Materials:

Reliable media to store assignments.

Attendance:

Attendance is important especially for this class. You cannot participate if you are not in attendance. Unexcused cuts in excess of 3 may result in a reduction of 10 % in class participation grade for every cut in excess of 3. Thus if you miss 5 classes your class participation grade will be a maximum of 80%. Also, it is unlikely you will be successful in class assignments, tests, or projects. In addition, after 5 absences, a deduction of 5% per absence may be deducted from your final grade. There are no exceptions to this attendance rule except with the approval of the instructor. The instructor reserves the right to reject all such requests. Lateness is disruptive and may result in a similar penalty.

You are expected to read all chapter material prior to the scheduled class. For testing, you will be responsible for all material covered in class as well all projects and assigned text chapters. It is imperative that you attend all scheduled classes. **Material will be covered in class that is not in the texts.**

This class may involve hands-on time learning to use various software packages. In case of unavoidable absence, special effort on the part of the student is a necessity. Due to the cumulative nature of work done, students are expected to find out about material missed *outside* of class time and *before* the next class, so that normal progress in class can resume. Due to the amount of material we will cover, very little time can be spent reviewing material already covered.

Research Projects and Presentations:

During the semester, students will have the opportunity to participate in team and individual projects. Students will be required to research topics beyond those covered in the course text to complete some project requirements. Students will be required to evaluate themselves and fellow team members. Grades for these projects will be based on the successful completion of stated project criteria and student evaluation feedback. At the end of project, students are required to make a formal presentation about results of their work, problems encountered, and their approach to solving the problem.

Course Grading:

The purpose of a grade is to give students feedback on the degree of their success in assimilating course content. In IST452, the following grading scale has been adopted and will hopefully provide each student with the opportunity for a good grade. The following grading structure is based on the required plus/minus system of the University.

A	94 - 100
A-	90 - 93
B+	87 - 89
B	84 - 86
B-	80 - 83
C+	75 - 79
C	70 - 74
D	60 - 69
F	59 and below

Grade Breakdown:

All final grading will be the responsibility of the Instructor with general weighting given below. The syllabus is subject to change.

Tests/Quizzes	25%
Class Participation	25%
Blog participation/In-class assignments	50%

The primary goal of the IST program is to build leaders for a digital global economy. This is best achieved through active learning. Class discussion, assignments, and presentations are designed to develop your oral, written, and critical thinking skills. Leaders require all these skills in today's economy.

General Grading Rubric

Product, Project, or Assignment	Very Poor or Absent	Below Avg.	Satisfactory	Good	Excellent
1. Mechanics of writing, grammar, punctuation	0	2	3	3.5	4
2. Organization and structure	0	2	3	3.5	4
3. Creativity and/or insight	0	2	3	3.5	4
4. Demonstrates knowledge	0	2	3	3.5	4

General Term Schedule (subject to changes):

Week	
Jan 12	Introduction, Intro to eLaw
Jan 19	e-Law
Jan 26	e-Law
Feb 2	e-Law
Feb 9	Privacy
Feb 16	Privacy
Feb 23	Privacy
Mar 2	Privacy
Mar 9	Privacy
Mar 16	Privacy
Mar 23	Security
Mar 30	Security
Apr 6	Security
Apr 13	Security
Apr 20	Security
Apr 27	Security
May 4	No final

IST 452 Projects:

Blogi

The course will involve creation of Blogs that will serve as a comprehensive documentation of our semester long exploration. Participation will be frequent and required. Grading will be based on the general grading rubric.

In-class Assignments

Each week we may spend a portion of class with discussion activities including cases, models, standards, exercises or programs. Some may involve individual activities and some may be group activities. This is a very important part of our course. If you miss class you still must complete the in-class assignment. If you must miss a class, you need to obtain instructions and materials from a fellow classmate. In addition, you are expected to keep up to date on current events. Individuals may be selected to read and discuss an appropriate current event for class.

Assignment Submission:

In general assignments will be submitted electronically through ANGEL. Also in general, assignments will be posted in ANGEL. http://cms.psu.edu

Discussion Activities:

Each week we may spend a portion of class with discussion activities. These may take the form of in-class assignments, review of homework, discussions and/or presentations. Some may involve individual activities and some may be group activities. These are required and will be included in the class participation grade. All homework must be done prior to class on the scheduled due date.

Homework:

Students will be assigned homework problems from the course text or supplemental source. All assignments that are not submitted by the specified due date will receive a penalty.

Course Rules:

Mutual respect and courtesy is required.

There will be no Internet surfing, Instant Messaging, text messaging, or email correspondence allowed during class. All cell phones and pagers must be turned off or to silent position. Violation of this policy will result in significant reduction in class participation and in-class assignment grades. There may be times when these activities will be permitted. These times will be clearly stated.

If you have any questions, please email me through my PSU email account not through ANGEL email. If you must miss a class, you need to obtain instructions and materials from a fellow classmate.

Text chapters and assigned outside readings will be expected prior to class to facilitate learning and class discussions.