

DISS 790 – Information Policy: Assignment D
Intellectual Property/E-Commerce Regulatory Environment
National Security/Cybercrime

by

Ronald G. Wolak
wolakron@nova.edu

A paper submitted in fulfillment of the requirements
for DISS 790 – Information Policy: Assignment D

School of Computer and Information Sciences
Nova Southeastern University

December 2000

An Abstract of a Paper Submitted to Nova Southeastern University in Fulfillment of the
Requirements for DISS 790 – Information Policy: Assignment D

DISS 790 – Information Policy: Assignment D
Intellectual Property/E-Commerce Regulatory Environment
National Security/Cybercrime

by
Ronald G. Wolak

December 2000

The paper that follows was submitted to satisfy the requirements of DISS 790 – Information Policy: Assignment D. In the following pages, the paper completed nine tasks related to intellectual property, e-commerce regulatory environment, national security, and cybercrime.

Table of Contents

Abstract	ii
1. Task 1	1
2. Task 2	5
3. Task 3	7
4. Task 4	12
5. Task 5	18
6. Task 6	23
7. Task 7	30
8. Task 8	36
9. Task 9	42

Task 1

What are the major differences between a copyright and a patent?

Copyrights differ from patents in several ways. These differences include the type of intellectual property protected, breadth of protection, period until protection takes effect, length of protection, cost of the application process, application time limits, right to protect improvements, and maintenance fees charged to continue coverage.

Type of Intellectual Property Protected

The basic difference between a copyright and a patent is the type of intellectual property each protects. A patent protects ideas as expressed in an invention (e.g. a machine or process) (Fishman, 2000). In contrast, a copyright protects only the words an author uses to express an idea, not the idea itself. A copyright covers only the expression of a work. It does not prevent people from appropriating ideas that the work embodies (Oppedahl & Larson, 2000b).

Immediate Protection

Another major difference is the period it takes for protection to take effect (Strong, 1999). Copyright protection begins the moment a work is created and fixed in a tangible form. In addition, copyright registration is routinely granted upon filing a simple application. Patent coverage, on the other hand, is granted only after preparing a detailed application, and then only after an examiner determines the application is allowable. In addition, the patent application process can take years to complete, and often ends with rejection.

Breadth of Protection

In addition, patents are more narrowly defined than copyrights (Karjala, 1998).

Patents are narrowly claimed, and the protection afforded by a patent is limited to those claims. Copyrights, on the other hand, have no requirement for the owner to specify which aspects of a work are protected and which are not.

Length of Coverage

The length of time that a copyright remains in effect is considerably longer than that of a patent. For example, the term of a utility patent is either 17 or 20 years (Alpern, 1999). In contrast, copyright protection for works created after January 1, 1978 remains in effect for 95 years from publication or 120 years from creation, whichever is shorter.

Cost

Cost is another area in which the two are different (Oppedahl & Larson, 2000a). In addition to being complicated, the patent process is expensive and can cost \$10,000 or more. In contrast, the filing fee to register a copyright is only \$30.

Application Time Limits

Under U.S. patent law, a patent will not be granted unless the application is filed less than one year from the date that the invention was sold or offered for sale within the United States (Oppedahl & Larson, 2000b). In addition, the patent will be denied unless the application is filed within one year of the date the invention was described in a printed publication anywhere in the world.

In contrast, a copyright application may be filed many years after the initial publication of the work (Oppedahl & Larson, 2000a). There is no particular time limit imposed for filing a copyright registration application.

Right to Protect Improvements

Copyrights and patents also differ in the area of improvements (Karjala, 1998). A copyrighted work may not be improved without the owner's permission. In contrast, another person may file for and receive a patent for improvements made to another invention.

Maintenance Fees

Another difference between copyrights and patents is the requirement to pay maintenance fees throughout a patent's life (Oppedahl & Larson, 2000b). Failure to pay these fees, which add up to thousands of dollars, results in patent expiration. No maintenance fees are required for a copyright.

Conclusion

In summary, many differences exist between copyrights and patents. Major differences include the type of intellectual property protected, breadth of protection, period until protection takes effect, length of protection, cost of the application process, application time limits, right to protect improvements, and maintenance fees charged to continue coverage. Finally, the most fundamental difference is that patents protect creative, functional invention, while copyrights protect creative, nonfunctional authorship (Karjala, 1998).

References

- Alpern, A. (1999). *101 Questions About Copyright Law*. Mineola, New York: Dover.
- Fishman, S. (2000). *The Copyright Handbook: How to Protect and Use Written Works* (Fifth ed.). Berkeley, CA: Nolo.
- Karjala, D. (1998). The Relative Roles of Patent and Copyright in the Protection of Computer Programs. *John Marshall Journal of Computer & Information Law*. <http://www.jmls.edu/jcil/17/karjala.html>. Accessed December 6, 2000.
- Oppedahl, C., & Larson, M. (2000a). General Information About Copyrights. *Oppedahl*

& Larson LLP. <http://www.patents.com/copyrigh.htm>. Updated September 13, 2000. Accessed November 24, 2000.

Oppedahl, C., & Larson, M. (2000b). General Information About Patents. *Oppedahl & Larson LLP*. <http://www.patents.com/patents.htm#compare-copyright>. Updated May 13, 1997. Accessed November 24, 2000.

Strong, W. (1999). *The Copyright Book: A Practical Guide* (Fifth ed.). Cambridge, Massachusetts: MIT Press.

Task 2

Subtask a - Which of the following elements of information must be used on a copyright notice: Copyright symbol, Name of owner, Year of first writing, Words: "All rights reserved"

Answer:

Copyright symbol

Name of owner

Year of first writing

A properly constituted copyright notice has all of the following elements: the C in a circle symbol, or the word copyright, or the abbreviation "Copr.", the name of the copyright owner, and the year of first publication (Strong, 1999). The phrase "All rights reserved" is not required. In addition, filing for a copyright is not required.

Subtask b - Which of the following types of works can be copyrighted? Titles of books, Computer programs, Mathematical formulas, Musical recordings, Sculptures

Answer:

Computer programs

Musical recordings

Sculptures

Copyright protects "original works of authorship" (U.S. Copyright Office, 2000a). These works must also be fixed in a tangible form of expression. Copyright works include the following: literary, musical, dramatic, pantomimes and choreographic, pictorial, graphic, sculptural, motion pictures, sound recordings, and architectural. Titles, names, short phrases, and slogans are not protected. In addition, mathematical formulas are not protected (Strong, 1999). Mathematical equations are regarded as common

property, as are scientific discoveries, and historical theories.

However, there may be a basis for copyright protection when a recipe or formula is accompanied by substantial literary expression in the form of an explanation or directions (U.S. Copyright Office, 2000c). Furthermore, there appears to be a trend in the U.S. Patent Office to grant patents to algorithms where a machine (i.e. computer) is identified as a component (Strong, 1999). For example, a patent was granted to an algorithm developed by Bell Labs. The algorithm can be used to optimally route anything from airline flights to telephone calls.

References

- Strong, W. (1999). *The Copyright Book: A Practical Guide* (Fifth ed.). Cambridge, Massachusetts: MIT Press.
- U.S. Copyright Office (2000a). Circular 1: Copyright Basics. *Library of Congress*. <http://www.loc.gov/copyright/circs/circ1.html>. Updated May, 2000. Accessed December 3, 2000.
- U.S. Copyright Office (2000c). Questions Frequently Asked in the Copyright Office Public Information Section. *Library of Congress*. <http://www.loc.gov/copyright/faq.html>. Updated June 2, 2000. Accessed December 3, 2000.

Task 3

Answer the following statements concerning copyright as true or false. Several of the statements may require elaboration beyond a true/false answer.

Subtask a - "A copyrightable work first becomes protected by copyright law when it is imagined."

False, a copyrightable work first becomes protected by copyright law when it is "fixed in a tangible form" (U.S. Copyright Office, 2000a).

Subtask b - "Anything posted to newsgroups or discussion forums on the net are in the public domain."

False, a newsgroup or discussion forum posting is not in the public domain unless the author/owner of the posting has dedicated it to the public or the copyright term of the posting has expired (Oppedahl & Larson, 2000a).

Subtask c - "I can adapt another's work and seek a copyright for the resulting publication."

False, only the owner of the copyright for a work has the right to authorize someone else to adapt or create a new version of the work (U.S. Copyright Office, 2000c). In addition, an adaptation of another's work is not original and therefore not copyrightable.

Subtask d - "I can copy anything as long as it doesn't have a copyright notice."

False, the use of a copyright notice is not required under U.S. law (optional for works published on or after March 1, 1989) (Chabrow, 1996). Copyright law protects a copyrightable work as soon as it is fixed in a tangible form (U.S. Copyright Office, 2000a). While using a copyright notice was once required by prior law, it is now optional.

Subtask e - "I can make copies of anything as long as I don't make money in doing so."

False, section 106 of the 1976 Copyright Act generally gives the owner of a copyright the exclusive right to reproduce or authorize others to reproduce the work in copies or phonorecords (U.S. Copyright Office, 2000a). This exclusive right is limited in cases in which the copying meets "fair use" factors.

Subtask f - "Copyright is simply too costly to bother."

False, copyright registration is inexpensive and offers many benefits to the owner (Oppedahl & Larson, 2000a). For example, it creates the presumption of ownership and is required in order to bring a lawsuit for infringement of a U.S. work. In addition, the filing fee to register a copyright is only \$30.

Subtask g - "I can repost someone's email to me without violating copyright."

False, the instant someone finishes typing an e-mail it is protected by federal copyright law (Overly, 1999). Sending an e-mail to someone gives that person the right to make a copy of it on his/her hard disk drive. It does not give that person permission to forward the message to a wide number of people, post the message on the Internet, or incorporate it into another work. However, depending on the circumstances, the sender may have given permission to forward the message to someone else.

Subtask h - "I can't get arrested for copyright infringement as long as the value of what I am copying is \$500 or less."

True, because the total retail value of the copyrighted work must be more than \$1,000 for the violator to be prosecuted criminally (Fishman, 2000). In addition, copyright infringement has traditionally been dealt with in civil court and does not

involve arrest.

Subtask i - "I don't have to worry about copying and distributing copyright materials for educational purposes. Such materials are exempt under U.S. copyright law's 'fair use doctrine'."

False, while “fair use” does limit the exclusive rights of a copyright owner when a work is copied and distributed for educational purposes (including multiple copies for use in the classroom), educators must consider the following factors to determine if their actions are covered by “fair use” (Fishman, 2000):

1. The purpose and character of the use – including if it is to be used for nonprofit or commercial educational purposes
2. The nature of the copyrighted work
3. The amount of the work used in relation to the work as a whole
4. The effect of the use on the value of or the potential market for the work

The above factors do not weigh equally in every case. However, the courts when deciding fair use cases consider them all. Finally, the photocopying of limited portions of written works by teachers for classroom use is considered fair use.

Subtask j - "I have placed a copyright on my name."

False, titles, names, short phrases, and slogans are generally not eligible for federal copyright protection (U.S. Copyright Office, 2000a).

Subtask k - "If you don't defend your copyright, you will lose it."

False, a work is copyright protected from the moment it is created and fixed in a tangible form (U.S. Copyright Office, 2000a). The copyright remains in force until it expires. Expiration dates are determined by factors such as the creation date of the work,

the life span of the author, and if it was published or registered - not whether the copyright is defended.

Subtask 1 - "My use of someone else's original document is serving as a free advertisement for their publication and is not in violation of copyright laws."

False, using someone else's original document without authorization is a violation of U.S. copyright law (U.S. Copyright Office, 2000c). There are limited circumstances, under the fair use doctrine, where a sample or quote may be used without permission. However, providing free advertisement is not one of them.

References

- Chabrow, E. (1996). Five Major Myths of Copyright Law. *InformationWeek*.
<http://www.techweb.com/se/directlink.cgi?IWK19960325S0047>. Updated March 25, 1996. Accessed November 24, 2000.
- Fishman, S. (2000). *The Copyright Handbook: How to Protect and Use Written Works* (Fifth ed.). Berkeley, CA: Nolo.
- Oppedahl, C., & Larson, M. (2000a). General Information About Copyrights. *Oppedahl & Larson LLP*. <http://www.patents.com/copyrigh.htm>. Updated September 13, 2000. Accessed November 24, 2000.
- Overly, M. (1999). *E-policy: How to develop computer, e-mail, and Internet guidelines to protect your company and its assets*. New York: American Management Association.
- U.S. Copyright Office (2000a). Circular 1: Copyright Basics. *Library of Congress*.
<http://www.loc.gov/copyright/circs/circ1.html>. Updated May, 2000. Accessed December 3, 2000.
- U.S. Copyright Office (2000c). Questions Frequently Asked in the Copyright Office Public Information Section. *Library of Congress*.
<http://www.loc.gov/copyright/faq.html>. Updated June 2, 2000. Accessed December 3, 2000.

Task 4

What remedies are there for the problems that are seemingly plaguing the U.S. patent system?

A significant number of intellectual property experts believe that the U.S. patent system is under more strain today than during any other period in its history (Lepkowski, 2000). The problems that plague the system come from many sources and are related to developments in biotechnology, information technology, and Internet-based business processes. As a result, the intellectual property courts, along with the U.S. Patent and Trademark Office (USPTO), are overloaded with new challenges that have little or no precedent.

The following sections discuss problems the PTO must address along with possible remedies. The problems include unqualified patent examiners, lack of resources and tools, patentability of software and software-enabled business methods, low standards/overstated claims, high patent fees, and lengthy times to patent.

Problems

Unqualified Patent Examiners

In general, patent examiners are not sufficiently familiar with new technologies. Examiner inexperience often results in the issuance of patents with claims that are too broad. In addition, unqualified examiners contribute to the PTO's biggest problem of not being able to locate "prior art" (Heckel, 1992). In addition, one of the biggest challenges facing PTO examiners is to gain experience in handling the increasing number of business method patents (Lepkowski, 2000). For example, a competent examiner could have blocked the Compton multimedia patent since the patent's claims covered techniques that are well known to any knowledgeable computer programmer.

Lack of Resources and Tools

Not only are many of the PTO's patent examiners unqualified, there are also not enough of them to handle the increasing workload. The shortage of examiners is primarily caused by attrition and a lack of funding. For example, the PTO encourages its examiners to take law courses to improve their job skills (Garfinkel, 1994). However, patent examiners routinely leave government service once they earn their law degrees.

In addition, current funding from Congress does not allow the PTO to issue patents in a timely manner (Fisher, 1997). The PTO's average patent pendency is now set at 20 months with complicated technology patents taking even longer. Lack of funding also limits the wages the PTO is able to pay examiners. Patent examiners currently earn from one quarter to one third that of an industry engineer.

A lack of tools further hinders the PTO's inexperienced examiners (Ratliff, 2000). For example, a searchable, centralized database would enable examiners to more effectively screen out inventions that are not novel.

Patentability of Software and Software-enabled Business Methods

In recent years, the area of intellectual property related to the software programming that enables business methods has become controversial (Lepkowski, 2000). It began with the Federal court of Appeals' 1998 decision in *State Street Bank & Trust Co. versus Signature Financial Group* (Bresnahan, 2000). The court found in favor of Signature and upheld its business method patent. The patent covered a data processing software system that performed a set of elaborate calculations required to maintain a complex investment portfolio.

Examples of other business method patents that have been in the courts recently are Amazon.com's one-click ordering system and Priceline.com's Web-based reverse auctions (Pressman, 2000). Congressional critics and patent attorneys charge that the PTO's research methods, which rely on limited information, fail to turn up evidence of business methods that are widely in use online.

In addition to the new problems created by software-enabled business method patents, ordinary software patents present a fundamental problem because any programmer can unknowingly violate them. What may seem to be a trivial section of code to a programmer may already be a patented routine (Garfinkel, 1994). In addition, conducting a patent search is not an adequate solution since it is costly, time consuming, and does not conclusively determine if any existing patents have been violated.

Low Standards/Overstated Claims

The Compton's patent is a classic example of overstated claims in a software patent (Ratliff, 2000). The patent covered a common CD-ROM search method, and Compton's threatened to exact licensing fees from any company developing multimedia CDs. The controversy that followed led to the reexamination and rejection of the patent by the PTO.

High Patent Fees

High patent fees significantly limit the ability of inventors and companies, particularly the small inventor, to take part in the patent system (Fisher, 1997). For example, a patent search can cost between a few hundred and a few thousand dollars (Garfinkel, 1994). In addition, the cost of a patent lawsuit averages \$1.5 million (Lepkowski, 2000).

In the future, reduced levels of Congressional funding will most likely result in even higher patent fees (Fisher, 1997). Without sustained levels of funding, the PTO will be unable to cover operating costs and will be forced to raise user fees – thereby decreasing the number of inventors able to gain access to the U.S. patent system.

Lengthy Times to Patent

The length of time to finish a patent examination is another problem. Overloaded patent examiners sometimes take years to finish the process. In industries with short innovation cycles, this can have a negative effect. For example, the software industry has only an 18-month innovation cycle (Lepkowski, 2000). Thousands of existing software patents will probably not hold up to litigation because the shorthanded PTO did not have enough time to conduct an adequate search of the prior art.

Remedies

Central Library

The ideal patent office would include a huge, centralized, and searchable database of prior art that examiners could use to review applications (Ratliff, 2000). Existing patent fees (currently being diverted by Congress to other projects) could fund this central library. The existing system gives patent examiners a limited amount of time to sort through stacks of paper and use an outdated computer system to review each patent. In the case of industries with short innovation cycles, a searchable, central library would be of even greater benefit.

Probation Period

Even with a central library, patent examiners will be unable to match the resources available to industry experts and venture capitalists. Another remedy would be

to take advantage of these private sector resources to improve the quality of patents. Under one proposal, a formal opposition period would be set up before a patent is granted. During this period, “probational” patents would be posted on the Internet for the vast audience of interested parties to look over for potentially overstated claims (Ratliff, 2000). This additional opportunity to challenge the award of questionable patents (e.g. some business method patents) would simplify the whole process (Ellis, 2000).

Bonus System

In conjunction with a probationary period, another positive step would be to link the bonuses received by patent examiners with the number of issued patents that survive the formal opposition period (Ratliff, 2000).

Appropriate Levels of Public and Private Funding

Another remedy for the problems facing the PTO would be to provide adequate public and private funding (Fisher, 1997). Patent fees (currently diverted by Congress to a general fund) should be earmarked for the PTO. In addition, Congress should fully fund the PTO’s public functions, such as classifying, archiving, indexing, maintaining the patent library, and general administration. Individual users should pay reasonable fees for the PTO’s private functions, such as patent application processing and other individual requests. Additional funds could also be used to give patent examiners higher wages as well as training in areas of new technology.

Conclusion

Perhaps the greatest obstacle to change at the PTO is inertia (Ratliff, 2000). Since the first patent issued in 1790, few people have paid much attention to the patent office. Today the PTO faces numerous problems related to unqualified patent examiners, lack of

resources and tools, patentability of software and software-enabled business methods, low standards/overstated claims, high patent fees, and lengthy times to patent. Remedies for these problems include a central library, a formal opposition period, an examiner bonus system, and appropriate levels of public and private funding.

References

- Bresnahan, J. (2000). Choose Your Poison. *CIO Magazine*.
http://www.cio.com/archive/041500_poison.html. Updated April 15, 2000.
 Accessed November 24, 2000.
- Ellis, K. (2000). Net Patent Bill Introduced. *WiredNews*.
<http://www.wired.com/news/politics/0,1283,39238,00.html>. Updated October 3, 2000. Accessed December 9, 2000.
- Fisher, D. (1997). Statement by Daniel E. Fisher, IEEE Chair. *IEEE*.
<http://www.ieeeusa.org/documents/FORUM/LIBRARY/PAPERS/hr673.html>.
 Updated February 26, 1997. Accessed December 7, 2000.
- Garfinkel, S. (1994). Patently Absurd. *WiredNews*.
http://www.wired.com/wired/archive/2.07/patents_pr.html. Updated July, 1994.
 Accessed December 7, 2000.
- Heckel, P. (1992). Debunking the Software Patent Myths. *ACM*.
<http://www.heckel.org/Heckel/ACM%20Paper/acmpaper.htm>. Updated June, 1992. Accessed December 7, 2000.
- Lepkowski, W. (2000). Rifts in U.S. Patent System Spur National Research Council to Undertake "Most Ambitious Exam Ever". *Research Technology Management*.
http://www.onlinejournal.net/iri/RTM/2000/43/3/html/43_3_2.html. Updated May 1, 2000. Accessed December 9, 2000.
- Pressman, A. (2000). The Great Patent Giveaway. *TheStandard*.
<http://www.thestandard.com/article/display/0,1151,20543,00.html>. Updated December 4, 2000. Accessed December 10, 2000.
- Ratliff, E. (2000). Patent Upending. *WiredNews*.
http://www.wired.com/wired/archive/8.06/patents_pr.html. Updated June 8, 2000.
 Accessed December 7, 2000.

Task 5

Briefly, outline the pros and cons of UCITA. Do you support passage of this law by state legislatures? Why/why not?

UCITA is the Uniform Computer Information Transaction Act. The National Conference of Commissioners on Uniform State Laws (NCCUSL) approved UCITA as a proposed uniform state law in July 1999 (Foster, 1999b). The proposed law governs all contracts for the development, sale, licensing, support, and maintenance of computer software (Kaner, 2000). In addition, UCITA extends to other contracts involving information and to the sales of computers, computer peripherals, and embedded software.

UCITA became law in Maryland on October 1, 2000. Software vendors, no matter where they (or their licensees) are located, are now able to cite Maryland law as their “choice of law” in a licensing contract (Thibodeau, 2000). One exception is Iowa, which recently passed legislation to protect in-state firms and residents from UCITA. Like Maryland, Virginia adopted the law but delayed implementation until next July.

Proponents of the law include the software publishing industry (Warren, 2000). In fact, several large computer companies are funding vigorous lobbying efforts to have UCITA enacted nationwide. Opposition to the legislation is extensive. A partial list includes the Attorneys General from half the states, the Federal Trade Commission (FTC), the American Association of Law Libraries, the ACM (Association for Computing Machinery), and the American Bar Associations’ Working Group on Consumer Protection.

Cons

Critics of UCITA say the law gives vendors too much control (Kaner & Pels, 1999). Under UCITA, software publishers have no duty to provide a virus free product.

In fact, software vendors can avoid paying for damages caused by a virus by including a simple disclaimer of implied warranties to their licensing agreement. Critics also point out that consumers are only able to see the licensing agreement after they have bought the product. No other industry in the U.S. is allowed to enforce post-sale warranties.

Critics also cite the following:

- UCITA authorizes vendors to disable automatically or “repossess” their software on a given date unless a license renewal fee is paid and registered. For example, a vendor could send a message to a computer to shut down a copy of its software. For business critical applications, this could shut down a company. This form of electronic self-help would be a “gun to the head” of corporate customers when disputes arise (Foster, 1999a).
- UCITA’s endorsement of shrink-wrap licenses will make unfair terms enforceable in court.
- The cost of negotiated contracts will increase because of UCITA. UCITA defaults favor software publishers. This will force corporate customers to negotiate from a weaker position.
- New UCITA vendor friendly rules conflict with other state, federal, and international efforts to bring order to the Internet. The law creates less uniformity of law rather than more.
- The added protection provided to the software industry by UCITA will be a disincentive to improve existing software applications and will also encourage the premature release of bug-ridden products.

- UCITA could allow publishers to outlaw all forms of reverse engineering. Reverse engineering is often key to making applications interoperable.
- The law redefines “material breach of contract” and makes it harder to return defective products. For example, a software publisher could include a clause in their shrink-wrap contract that stipulates the licensee cannot cancel the contract and demand a refund even if the product is worthless (Kaner & Pels, 1999).
- UCITA allows vendors to charge users a non-refundable per-minute fee for technical support. This fee could apply even when the support is for a defect that was known at the time of shipment.
- The law also authorizes restrictions that make it harder for consumers to obtain third-party maintenance or to transfer the software to another user.
- UCITA provides loopholes that would allow software publishers to have legal actions decided in their state rather than the consumer’s state.

Finally, concerns over UCITA have been raised by half of the State Attorneys General (Spears, 2000). They argue that the pre-emptive aspects of UCITA eviscerate a variety of state consumer protection laws.

Pros

Proponents of the act argue that UCITA is needed to insure continued growth (Spears, 2000). The law they say lets end users and vendors agree to any contract terms they want. In fact, NASDAQ’s vice president and general counsel stated that UCITA would bring certainty to NASDAQ’s online contracting by providing clear guidelines.

Proponents also cite the following (Brennan & Barber, 1999):

- UCITA would provide standardization. The legal standards for information contracting are currently in disarray.
- Since commercial contract law is made by the states, not the federal government, UCITA would provide uniformity (i.e. provide the single set of uniform rules needed to realize the potential of e-commerce).
- UCITA would also stimulate innovation by encouraging software developers to bring experimental products to market by allowing them to control their risks with disclaimers.

Finally, proponents argue that without UCITA significant problems will occur. These include the increased legal cost of having to comply with different local codes and reduced competition since small companies will not be able to afford these costs.

Conclusion

State legislatures should not pass UCITA. A cardinal rule of intelligent legislation is, “If it ain’t broke, don’t fix it” (Spears, 2000). Software publishers and customers will be better off if the courts are allowed to decide software license issues on a case-by-case basis. UCITA is one-sided and heavily favors the software industry (e.g. software repossession and the enforceability of unfair contract terms).

Furthermore, UCITA would validate existing shrink-wrap licenses and protect companies from users of software that was poorly tested and debugged (Foster, 1999c). Under UCITA, a software publisher is granting the consumer a license to use its product. It is not a sale. Therefore, the user must agree to waive any and/or all rights if he/she wishes to use the software. UCITA is not needed. Proponents of the law fail to recognize

that courts across the country have enforced “reasonable” shrink-wrap licenses in the past.

References

- Brennan, L., & Barber, G. (1999). Why Software Professionals Should Support UCITA. *Software Quality Professional*. http://sqp.asq.org/vol1_issue4/sqp_v1i4_brennan.html. Updated August 1999. Accessed December 14, 2000.
- Foster, E. (1999a). UCITA: Top Issues. *InfoWorld*. <http://www.infoworld.com/cgi-bin/displayStory.pl?features/990531ucita3.htm>. Updated August 30, 1999. Accessed December 12, 2000.
- Foster, E. (1999b). What is UCITA? *InfoWorld*. <http://www.infoworld.com/cgi-bin/displayStory.pl?features/990531ucita1.htm>. Updated August 30, 1999. Accessed December 12, 2000.
- Foster, E. (1999c). Why is UCITA Important? *InfoWorld*. <http://www.infoworld.com/cgi-bin/displayStory.pl?features/990531ucita2.htm>. Updated August 30, 1999. Accessed December 12, 2000.
- Kaner, C. (2000). Uniform Computer Information Transactions Act (UCITA). *Badsoftware.com*. <http://www.badsoftware.com/uccindex.htm>. Updated September 16, 2000. Accessed December 13, 2000.
- Kaner, C., & Pels, D. (1999). UCITA: A Bad Law That Protects Bad Software. *NetworkWorldFusion*. http://www.nwfusion.com/archive/1999/64142_05-03-1999.html. Updated May 5, 1999. Accessed December 14, 2000.
- Spears, M. (2000). Software Law From Hell. *UpsideToday*. <http://www.upside.com/texis/mvm/print-it?id=38fe2a930&t=/texis/mvm/news/news>. Updated May 2, 2000. Accessed November 24, 2000.
- Thibodeau, P. (2000). Maryland's UCITA May Have National Reach. *Computerworld*. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO49486,00.html. Updated September 4, 2000. Accessed September 12, 2000.
- Warren, J. (2000). UCITA "Rules". *Government Technology*. <http://www.govtech.net/publications/gt/2000/sept/eComerceSL/stateLocal.phtml>. Updated September, 2000. Accessed December 2, 2000.

Task 6

Should e-commerce be exempt from sales tax? Why/why not?

In 1998, the Internet Tax Freedom Act (ITFA) became law (Pressman, 2000). ITFA defines electronic commerce (e-commerce) as “any transaction conducted over the Internet or through Internet access, comprising the sale, lease, license, offer or delivery of property, goods, services or information, whether or not for consideration, and includes the provision of Internet access” (Bartlett, 2000). The law which is set to expire in October 2001, prohibits the imposition of any sales or use taxes on Internet access or any discriminatory or multiple taxes on electronic commerce.

A grandfather clause in the act gives states that taxed Internet access on or before October 1, 1998, the right to continue the practice (Rogers, 2000). As a result, Iowa, North Dakota, South Dakota, Connecticut, New Mexico, Ohio, Tennessee, South Carolina, Texas, and Washington currently tax Internet access. However, a bill to extend the current moratorium to 2006 is currently making its way through Congress. If the moratorium becomes law, the grandfather provision will end.

Under existing tax laws that remain in effect until the federal moratorium expires, e-commerce businesses are subject to the same guidelines that apply to catalog businesses (Tessler, 2000). Under those rules, from the 1992 Supreme Court decision in *Quill Corporation versus North Dakota*, merchants do not need to collect sales taxes unless they have a “nexus” (i.e. physical presence such as a store or warehouse) in the state in which a customer is located. In addition, it is important to note that e-commerce is merely an extension of mail and catalog sales and are treated the same for tax purposes.

Historically, states have had a difficult time taxing mail order sales (Bartlett, 2000). Unless the seller withholds the tax, the tax is usually not collected. In fact, several Supreme Court cases have made it difficult for states to force out-of-state sellers to withhold sales taxes. Generally, a business without a physical presence in a state is not required to withhold use taxes.

In order to avoid having to withhold sales taxes, some businesses have set up subsidiaries to handle Internet sales in order to avoid creating a nexus in a state (Bartlett, 2000). For example, Barnesandnoble.com is independent of the brick-and-mortar Barnes & Noble Bookstores. Since the majority shareholder of Barnesandnoble.com is German publisher Bertelsmann AG, the online bookseller does not withhold use taxes.

Should e-commerce be exempt from sales tax?

Yes, for reasons that include the fragile condition of new e-commerce businesses, the negligible tax revenue that would be collected, e-commerce's distinguishing features, and the problems created when taxing e-commerce.

Fragile Condition

According to a recent BizRate.com survey, 75 percent of online buyers will buy less on the Internet if the goods are taxed (Pastore, 1999). The survey also found that a domestic tax on e-commerce could stifle the ability of U.S. companies to succeed in the global marketplace. Online customers do not recognize state borders and in some cases would make their purchases elsewhere in the world to obtain a discount.

When Congress passed the Internet Tax Freedom Act, it realized that the Internet needed time to grow to become a viable medium for commerce (Sommers, 2000). This would be impossible if e-commerce was subjected to various taxing regimes imposed by

the states. The Internet is inherently susceptible to multiple and discriminatory taxation in ways that traditional commerce is not. For example, a typical Internet transaction might route throughout the country and even throughout the world, and dozens of jurisdictions could attempt to tax the transaction.

Negligible Tax Revenue

Many state and local governments fear that the shift to e-commerce will lead to the erosion of state and local retail sales and use tax bases (Ginty, 1999). For example, Ohio said it lost \$150 million in 1999. However, a nationwide study by Ernst and Young found that uncollected sales and use taxes in 1998 rounded out to a mere \$179 million (i.e. one tenth of one percent of the state and local taxes) (Du Pont, 1999).

Various factors contribute to the limited impact of e-commerce on state and local taxes (Ginty, 1999). These include the estimation that the vast majority of e-commerce activity is nontaxed or is in-state business-to-business sales, and that business-to-consumer sales are primarily for intangible services (e.g. travel and finance services and the sale of nontaxable items such as groceries and prescriptions). In addition, no evaluations have been done of the money added to the economy by untaxed e-commerce activities. Areas receiving increased revenue include property taxes, capital gains taxes, and income taxes (Rogers, 2000).

Proponents of Internet taxation argue the current situation (i.e. unfair competition for traditional business and lost tax revenue) will become worse as Internet sales increase drastically in the future (Bartlett, 2000). However, Internet sales will not grow exponentially according to the Commerce Department, and total e-commerce accounts

for little over one-half of one per cent of retail sales. In addition, estimates of future growth of Internet consumer sales are diving along with the prices of dot-com stocks.

Distinguishing Features

Although e-commerce is often viewed in a similar light as the mail order and catalog business, it has many distinguishing features that make it difficult to tax under traditional concepts (Sommers, 2000):

- Computer-to-computer transactions rarely leave a paper trail.
- E-commerce transactions, particularly when electronic cash is used, can be anonymous.
- Anonymous transactions do not provide information, such as location of the buyer and the seller.
- E-commerce allows the electronic delivery of goods (e.g. CDs, books, and movies in digital form).
- E-commerce makes possible the combination of taxable and non-taxable goods, such as taxable goods with tax-exempt services (e.g. a software package with e-mail technical support).

Problems Created

The main tax problems caused by e-commerce relate to basis of charge, anonymity, definition of transaction, compliance, and enforcement (Dyer, 2000).

- **Basis of Charge:** Most states' and countries' tax systems have a combination of charges that relate to the profits earned by a business that resides within their jurisdiction or to the place at which goods are delivered to customers.

E-commerce is usually not tied to a location.

- **Anonymity:** The identities of the parties involved in an e-commerce transaction are often difficult to obtain. If encrypted, the transaction would be almost impossible to trace.
- **Definition of Transaction:** When data is transferred over the Internet, should the transaction be classified as a service, a delivery of goods, or the granting of a license for use? In addition, should the proceeds be taxed as royalties, proceeds of sale, or copyright license fees?
- **Compliance:** Since it is generally the responsibility of suppliers of goods and services to collect transaction taxes, suppliers would be required to shoulder the burden of verifying the nature of each transaction and the location of each buyer.
- **Enforcement:** The enforcement of tax systems requires the presence of a representative of the taxpayer in the state or country. Currently, there is no effective way for a state or foreign jurisdiction to enforce another state's or country's tax laws.

Furthermore, traditional methods of taxation rely on the ability to verify location and use treaties to balance tax without unduly restricting commerce (Fairpo, 1999). The Internet provides a different environment – one in which automated functions are able to perform significant business with little or no physical presence or activity. Once again, this leads to the issue of jurisdiction. In order to impose taxes, a taxing authority (e.g. country, state, or local government) must have jurisdiction over the taxpayers.

Conclusion

In conclusion, perhaps the best argument against an e-commerce sales tax has to do with the practical problem of administering and collecting such taxes (Pressman,

2000). Determining how much to collect and then collecting and sending the sales taxes imposed by thousands of local governments would be a monumental task. The administrative and financial burden imposed by e-commerce sales taxation would cripple most firms.

Finally, another argument against e-commerce taxation comes from Paul Misener, Vice President for Global Public Policy at Amazon.com (Tessler, 2000). Misener pointed out that there is no need to tax Internet sales since so many state and local governments are running budget surpluses. He considers Internet sales taxation as a solution in search of a problem.

References

- Bartlett, B. (2000, July 7). No to State Internet Taxes. *Human Events*, 56, 21.
- Du Pont, P. (1999). Is a National Sales Tax Next for the Internet? *IntellectualCapital.com*. <http://ic.voxcap.com/issues/issue257/item5725.asp>. Updated July 15, 1999. Accessed December 2, 2000.
- Dyer. (2000). E-Commerce: The Tax Consequences. *The Dyer Partnership Limited*. http://www.netaccountants.com/ecommerce_tax_02.html. Accessed December 2, 2000.
- Fairpo, A. (1999). Taxation of Electronic Commerce: Residence. *The Tax Journal*. <http://www.e-tax.org.uk/articles/residence.shtml>. Updated September 13, 1999. Accessed December 2, 2000.
- Ginty, M. (1999). Survey: E-Commerce Isn't Resulting in Lost Taxes. *E-Commerce News*. http://ecommerce.internet.com/ec-news/article/0,,5061_141721,00.html. Updated June 21, 1999. Accessed December 2, 2000.
- Pastore, M. (1999). Sales Tax Would Harm E-Commerce. *E-Commerce News*. http://ecommerce.internet.com/ec-news/article/0,,5061_202891,00.html. Updated September 17, 1999. Accessed December 2, 2000.
- Pressman, S. (2000, Summer). E-commerce, the sales tax, and equity. *Dissent*, 47, 49-52.
- Rogers, A. (2000, May 15). House approves extension of Internet taxation moratorium. *Computer Reseller News*, 3.

- Sommers, R. (2000). Taxation of E-Commerce. *Taxprophet.com*.
<http://www.taxprophet.com/hot/jan%202000.htm>. Updated January, 2000.
Accessed December 2, 2000.
- Tessler, J. (2000, September 24). The debate over Internet taxes starting to heat up.
Florida Times Union, pp. H-3.

Task 7

Given the global challenges to network security most western governments are formulating cooperative strategies to pursue international perpetrators and are planning for contingencies in the case of cyber attacks. Some experts argue that the only way to mitigate the impact of massive cyber attacks is for government to begin mandating security practices and protocols in the private sector. Do you believe such a policy should be pursued? Why/why not?

The term terrorism is usually applied to organized acts or threats of violence designed to intimidate opponents (Encyclopedia.com, 2000). The term, which dates from the Reign of Terror (1793 – 1794) in the French Revolution, has taken on additional meaning in the 21st century. Computer or cyber –terrorism is a widely used term. It covers anything from crackers using PCs to compromise government and financial institutions to the use of the Internet and private bulletin boards by terrorists to disseminate information (Cyber terrorism, 1997).

G8 Cyber-crime Summit

In response to the threat from cyber attack to their national information infrastructures, government officials from the eight most powerful and industrialized nations met recently to develop a coordinated plan to address cyber attacks (Brown, 2000). At the three-day summit, held in Paris, representatives from the Group of Eight (G8) countries (i.e. Canada, France, Italy, Japan, Russia, the United Kingdom, and the United States) broadly called for the regulation of the Internet by both industry and governments.

Proposals submitted at the conference included:

- Requiring Internet users to register to use the Internet
- Creating an international force of “cyberpolice”

- Forcing Internet service providers (ISPs) to store traffic data for up to three months
- Engineering a form of “caller ID” into the Internet to make it easier to track down Internet users
- Drafting a treaty that would require countries to pass laws against hacking, computer fraud, and online child pornography
- Setting penalties, preserving evidence, and establishing mechanisms for cooperation in international investigations

The overall goal of the summit was to produce a global agreement that would eliminate “Internet havens” where criminals could find the facilities to launch cyber attacks.

Convention on Cyber-crime

In a similar effort and after more than three years of work, the Council of Europe (COE) recently posted the 22nd draft of its Convention on Cyber-Crime (Luening, 2000). The intent of the treaty is to harmonize European laws against hacking, fraud, computer viruses, child pornography, and other Internet crime. In addition, the treaty seeks to establish common methods of securing digital evidence to trace and prosecute criminals.

While the treaty may have been drafted with good intentions, there are many areas of concern. For example, the pact could have a negative effect on the free flow of information and ideas (CNET, 2000). A provision that forces ISPs to store user activity data would threaten personal privacy and create a data pool that could be “mined” to identify dissidents and to persecute minorities. Another treaty section requires access to encryption keys. This would force people to incriminate themselves. Overall, the treaty grants increased surveillance powers to European police agencies.

The treaty's attempt to establish common, mutually agreed upon methods of securing digital evidence is commendable. New requirements to have trained personnel available around the clock are vital to track down cross-border cyber-criminals. In addition, the treaty provides a set of mutually agreed upon definitions of terms related to cyber-crime.

Many believe the new treaty runs contrary to established norms for the protection of the individual and that it improperly extends the authority of police. For example, the treaty's ISP data storage requirements are clearly at odds with the European Union's Directive on the Protection of Personal Data (EU, 1995).

The U.S has endorsed the main principles of this European effort to fight cyber-crime (Brown, 2000). In fact, many believe the U.S. is fixated on increased monitoring and making the Internet less anonymous instead of increasing security and giving law enforcement authorities the tools to detect and prosecute online criminals. In response, a 27-member coalition made up of the ACLU and Privacy International recently urged the Justice Department not to endorse the international pact (Wolf, 2000). The coalition pointed out that the pact could force police in the United States to conduct searches under the treaty "that don't respect the limits of police powers imposed by the U.S. Constitution."

Dependent and Vulnerable

Internet security has now become a major concern in the United States. The growth of e-commerce and the large quantities of information transferred over the Internet (e.g. medical information, stock transactions, banking, and military data) have

made the U.S. dependent on the Internet (Pleshaw, 2000). The U.S., with more than half of the world's Internet assets, is vulnerable to cyber-attack.

For example, during the first eight months of this year, there were more than 15,000 computer attacks reported to the Computer Emergency Response Team (CERT) (Build, 2000). Furthermore, the U.S. Defense Department acknowledges that 65 percent of the hacking attacks were able to penetrate some parts of its computer networks (Cyber terrorism, 1997). In addition, it is estimated that 120 countries are known to be creating information warfare techniques. The threat of cyber attack is reinforced by the fact that there are 1.3 million people in the world today with the skills to launch an attack against a public communications network (Ulsch, 2000).

Should the government pursue a policy of mandating security practices and protocols in the private sector?

No, the U.S. government should not mandate security practices and protocols in the private sector. The government's failure to secure its own servers and network infrastructure does not make it the best candidate to mandate security policy for private industry. For example, someone in the Russian military was able to send a Trojan inside the Department of Defense (Pleshaw, 2000). The program attached itself to a network printer and instructed it to send all print jobs to a printer in Moscow.

The bottom line is that both government and private industry have not made the investment necessary to secure the Internet from cyber attack (Ulsch, 2000). The information industry and the Federal government need to allocate the resources required to properly secure the Internet. The technology is available – it just needs to be applied.

Re-engineering the Internet and reducing anonymity and personal freedom are not required to reduce the threat of cyber attack.

In summary, the installation of the security software along with the continuous application of the latest security patches is all that is needed. Private industry has just as much to lose as the Federal government does from cyber attack. In the process of securing our national infrastructure, we must take care not to lose our basic freedoms as U.S. citizens. Overreaction on the part of government will not solve the problem - cooperation with Internet service providers (ISPs) and the rest of the private sector will.

References

- Brown, D. (2000). Governments Mull Net Crime Rules. *Interactive Week*.
<http://www.zdnet.com/intweek/stories/news/0,4164,2574592,00.html>. Updated May 22, 2000. Accessed December 21, 2000.
- Build. (2000, December 11). Attacks on the rise. *The Industry Standard*, 174-175.
- CNET. (2000). Global Net Crime Treaty Updated Amid Concerns. *Reuters*.
<http://news.cnet.com/news/0-1005-202-3664446.html>. Updated November 13, 2000. Accessed November 26, 2000.
- Cyber terrorism (1997). *Secure Computing*.
<http://www.westcoast.com/securecomputing/july/terrorism/terrorism.pdf>. Updated July, 1997. Accessed December 2, 2000.
- Encyclopedia.com. (2000). Terrorism. *Electric Library*.
<http://www.encyclopedia.com/articles/12749.html>. Accessed December 20, 2000.
- EU. (1995). Council Adopts Directive on Protection of Personal Data. *Cordis*.
http://dbs.cordis.lu/cordis-cgi/srchidadb?ACTION=D&SESSION=259172000-11-25&DOC=7&TBL=EN_NEWS&RCN=EN_RCN_ID:4581&CALLER=EN_UNI_FIEDSRCH. Updated July 26, 1995. Accessed November 25, 2000.
- Luening, E. (2000). European Council Moves Net Crime Treaty Forward. *CNET News*.
<http://news.cnet.com/news/0-1007-202-3785827.html>. Updated November 20, 2000. Accessed November 25, 2000.
- Pleshaw, G. (2000, December 11). Meet the enemy. *The Industry Standard*, 168-172.

Ulsch, M. (2000, November). Future tense. *Information Security*, 30.

Wolf, J. (2000). U.S. Embraces European Computer Crime Proposal. *Reuters*.
<http://washtech.com/news/regulation/5697-1.html>. Updated December 4, 2000.
Accessed December 22, 2000.

Task 8

Should private sector websites be required to be ADA compliant? Be sure to note the consequences of such a requirement or lack thereof.

According to the 1992 U.S. Census, an estimated 24.1 million people in the U.S. have a severe disability (PCEPD, 2000). Congress passed the Rehabilitation Act of 1973 to assist the disabled. Section 508 of the law mandated that the federal government take steps to ensure federal facilities were accessible to the disabled. As a follow-up, Congress passed the Americans with Disabilities Act (ADA) in 1990 to further improve accessibility. The ADA “prohibits discrimination on the basis of disability in employment, programs and services provided by state and local governments, goods and service provided by private companies, and in commercial facilities.”

The spirit of Section 508 was resurrected for technology industries in 1998 with the enactment of the Workforce Investment Act (Harler, 2000). Under the new law, section 508 was revised to include electronic and information technology equipment used by federal workers and the public in federal buildings. Technologies covered are software and Web-enabled applications, Web sites, telecommunications functions, video and multimedia products, transaction machines, and information kiosks (Recktenwald, 2000).

The Office of Management and Budget (OMB) recently approved and published the revised Section 508 accessibility standards (Matthews, 2000a). The regulations will take effect June 21, 2001 and cost federal agencies an estimated \$1 billion per year to comply (Matthews, 2000b). Once in effect, some see the federal regulations as the first step toward similar legislation covering private industry Web sites. In addition, it is almost certain that state governments will adopt regulations similar to Section 508 (Harler, 2000). This trickle down effect will then require compliance by state-funded

institutions (e.g. schools). Furthermore, the U.S. Department of Justice believes the ADA does apply to Web sites (Thibodeau, 2000).

America Online recently settled a lawsuit by the National Federation of the Blind that used the new law as its basis (Wagner, 2000). In the settlement, AOL agreed to continue its efforts to ensure that AOL 6.0 is compatible with screen reader assisting technology, which makes it accessible to users that are blind or have impaired vision. According to the CNet tech-news service, 98 percent of current Web sites are considered inaccessible to the disabled (Olson, 2000). In addition, 65 percent of 200 sites focusing on disability issues were not accessible.

Assuming Congress does not clarify the current situation, the applicability of the ADA to private sector Web sites will remain unclear until the courts further analyze the issue (Mason, 2000). The issue is complicated by the fact that no industry standard exists to govern the interoperability between assistive technology and Web sites.

The Justice department is attempting to speed up the process by filing lawsuits arguing that the ADA does apply to Web sites. However, in the case it brought against OKbridge, Inc., which operates Web-based bridge tournaments, a district court ruled in favor of OKbridge, in part because OKbridge was not a “place of public accommodation” under the ADA because there was no physical structure or facility.

Should Private Sector Websites Be Required to Be ADA Compliant?

There are valid arguments on both sides of this issue. Here are a few:

- Pro: Advocates for the disabled contend that the changes needed to allow full access are not costly and would not prohibit the uses of graphics (Seminario, 1999).

- Con: Opponents argue that the cost will be high and cite the \$1 billion per year estimate for federal Web site compliance.
- Pro: Advocates emphasize that the Constitution's guarantee of free speech has no bearing on the issue (Olson, 2000). The First Amendment may prohibit officials from restricting speech based on content, but in this case, the ADA controls everyone's speech alike, whatever the content.
- Con: Opponents disagree and argue that the application of the ADA in the private sector will restrict the rights of Internet users to select the verbal, audio, and visual palette and syntax in which they wish to communicate (Olson, 2000). Furthermore, the House of Representatives' subcommittee on the Constitution is closely monitoring the situation (Mason, 2000). In February, the subcommittee held oversight hearings on whether applying the ADA to Web sites would violate the First Amendment right of free speech.
- Pro: The number of sites that are accessible by the disabled is a small minority, and the trend is to make sites even more complex and thus decrease accessibility even further (Seminario, 1999). Advocates contend that the ADA will benefit all users by forcing the implementation of universal principles in Web page design (Minow, 1999). Users who wish to display images may do so, while others with slow modems will be able to display text only.
- Con: The threat of lawsuit after posting a non-compliant Web site will severely limit the number of Web pages (Olson, 2000). For example, companies and individuals without the money or expertise to comply with the guidelines will

simply not post their information. In addition, opponents insist a genuine “digital divide” will open up and the Internet would lose 90 percent of the free Web content within a week if the ADA standards for enforced legally. The result will be that the vast majority of Internet users will be deprived of useful information because a small minority could not use it.

- Pro: Many disabled-rights advocates insist their legal efforts will only press reasonable applications of the law and not an extreme approach to its enforcement (Olson, 2000).
- Con: The ADA allows (and possibly encourages) self-generated and entrepreneurial filing of complaints. For example, one lawyer in Florida recently filed 323 ADA related complaints on behalf of his 72-year-old uncle (Olson, 2000).

Conclusion

Private sector Websites should not be required to be ADA compliant. The application of the ADA in the private sector at this time would seriously affect the spontaneity, freedom, and rapid growth of the Internet (Olson, 2000). The benefits of the law for the disabled do not offset the negative impact it would have on non-disabled Internet users (e.g. the loss of First Amendment rights and extinguishing the current explosion of information found on the Internet today).

The conversion of thousands of federal Web pages beginning in June will provide valuable lessons learned to private industry (Recktenwald, 2000). In addition, many companies now realize that if they are selling to the federal marketplace ADA compliance will have to be addressed. The federal effort will help both the public and

private sectors determine the real cost and additional effort needed to develop ADA compliant Web sites. Until the results of the federal effort are in, the private sector should be left alone.

References

- Harler, C. (2000). Barrier-Free Access: Who's Gonna Pay? *Interactive Week*.
<http://www.zdnet.com/filters/printerfriendly/0,6061,2453242-35,00.html>. Updated March 2, 2000. Accessed November 24, 2000.
- Mason, M. (2000). Does the ADA Apply to the Web? *WTOonline.com*.
http://www.wtonline.com/vol15_no13/federal/1815-1.html. Updated September 25, 2000. Accessed October 3, 2000.
- Matthews, W. (2000a). Access Board Spells Out Standards. *Federal Computer Week*.
<http://www.fcw.com/fcw/articles/2000/1218/web-access-12-22-00.asp>. Updated December 22, 2000. Accessed December 24, 2000.
- Matthews, W. (2000b). Software Central to Accessibility Standards, Cost. *Federal Computer Week*. <http://www.fcw.com/fcw/articles/2000/1218/web-access2-12-22-00.asp>. Updated December 22, 2000. Accessed December 24, 2000.
- Minow, M. (1999). Does Your Library's Web Page Violate the Americans with Disabilities Act? *California Libraries*.
<http://www.librarylaw.com/ADAWebpage.html>. Updated April, 1999. Accessed December 2, 2000.
- Olson, W. (2000, May). Access excess. *Reason*, 32, 49-51.
- PCEPD. (2000). Basic Facts. *President's Committee on Employment of People with Disabilities*. <http://www50.pcepd.gov/pcepd/pubs/ek97/facts.htm>. Updated December 22, 2000. Accessed December 24, 2000.
- Recktenwald, J. (2000). Technology For the Disabled: What Does Federal Law Mean For IT? *TechRepublic*.
<http://www.techrepublic.com/article.jhtml?src=search&id=r00620000504rec01.htm>. Updated May 4, 2000. Accessed December 2, 2000.
- Seminario, M. (1999). 'Handicapped Access' Hits the Web. *ZDNN*.
<http://www.zdnet.com/zdnn/stories/news/0,4586,2243282,00.html>. Updated April 18, 1999. Accessed December 2, 2000.
- Thibodeau, P. (2000). Does Disabilities Act Apply to Cyberspace? *Computerworld*.
http://www.idg.net/crd__137933.html. Updated February 9, 2000. Accessed

December 24, 2000.

Wagner, J. (2000). AOL Settles Lawsuit. *ISP-Planet*. http://www.isp-planet.com/news/aol_settles.html. Updated July 27, 2000. Accessed December 24, 2000.

Task 9

Should the government mandate OSHA ergonomic standards for telecommuters and home offices? Why/Why not?

The Occupational Safety and Health Administration (OSHA) recently released the final version of workplace ergonomic standards aimed at reducing the number of repetitive-motion injuries (Thibodeau, 2000). Ergonomics as defined by OSHA is “fitting jobs to people,” and repetitive-motion injuries afflict many workers with jobs that require heavy computer use (Robins, 2000). Ailments include carpal tunnel syndrome, tendonitis, lower back pain, and sciatica. In fact, 1.8 million U.S. workers experience such musculoskeletal disorders (MSDs) annually. In addition, 600,000 people suffer injuries that require time off from work.

The new standards will affect more than 100 million workers and 6 million companies. Industry reaction to the new OSHA rules is not supportive (Thibodeau, 2000). For example, the National Association of Manufacturers in Washington said it would immediately take legal action to block the federal rules. The U.S. Chamber of Commerce immediately filed a lawsuit claiming the “mammoth ergonomics rule is incomprehensible and unconstitutional” (Trott, 2000).

Although the new OSHA rules do not specifically require companies to purchase certain kinds of computer and office equipment, companies with workers suffering from ergonomic-related injuries will be required to address the problems (Thibodeau, 2000). Some ergonomic experts consider outfitting an office for good ergonomics to be a small burden. In many cases, they say all that is required is to ensure that computer monitors are directly in front of employees or that mice are placed at the same level as keyboards.

Many disagree and claim that U.S. businesses will have to spend billions of dollars to comply (Trott, 2000). OSHA acknowledges the cost but argues that businesses will save money in the end by preventing MSDs and reducing long-term disability claims.

On November 15, 1999, OSHA issued a related advisory stating that telecommuters' home work areas must comply with OSHA's workplace safety regulations (Hayworth, 2000). In addition, the advisory covered those who do not telecommute but may occasionally perform work at home. However, the agency withdrew the advisory under intense pressure from all areas. Opponents to the application of OSHA ergonomic standard to telecommuters are quite vocal. The following are a few of the pros and cons:

Pros

- Advocates see OSHA's recommendations as addressing serious problems faced by employees in the workplace (Robins, 2000). They argue that some telecommuters face conditions of heating and lighting that do not exist in traditional workplaces and businesses should not profit from the situation.
- Proponents also cite existing formal agreements that many businesses have with their at-home workers (Robins, 2000). These companies often provide workers with computers and a list of approved furniture. This ensures the provision of ergonomically correct conditions without having to perform home inspections. For example, Merrill Lynch has had an occupational safety program to cover at-home workers for the past four years (Dorning, 2000). The company provides ergonomic specifications for office equipment and requires photographs of the

workspace. Telecommuters must also give their permission to inspect their at-home workspaces with 48 hours notice.

- Advocates also emphasize that businesses save considerable capital costs by using an at-home workforce, and these workers deserve the same legal protections provided to traditional workers (Robins, 2000).
- OSHA emphasizes that employers (to reduce legal liability) should exercise reasonable diligence to identify hazards associated with at-home work assignments (Koch, 2000).

Cons

- Opponents argue that the overall workplace injury and illness rate is currently at its lowest level since the Bureau of Labor Statistics began reporting the rate in 1970. They consider OSHA's ergonomic standards a solution in search of a problem (Robins, 2000).
- Critics also state that the 30-year-old OSHA law was designed to cover old-fashioned offices and factories and should not be applied to 21st century business (Robins, 2000). In addition, the cost to equip employees with materials and conditions equivalent to a traditional office would needlessly cost billions of dollars.
- Furthermore, opponents argue that the extension of ergonomic standards to telecommuters would be a gross violation of privacy and see OSHA spot inspections in the home as a definite possibility (Hayworth, 2000).
- Critics also point out that there is no consensus in the medical or scientific communities as to the causes or cures for repetitive stress injuries (Gilroy, 2000).

- Opponents also say the application of OSHA standards for at-home offices will be responsible for the elimination of many telecommuting jobs. Employers faced with the added expense and complexity of the regulations will rethink current telecommuting programs (Reuters, 2000).

Conclusion

The government should not mandate OSHA ergonomic standards for telecommuters and home offices. Employers have demonstrated their commitment to provide a safe workplace for employees and statistics bear this out. For example, workplace injuries have declined more than 24 percent since 1994 while the number of workers has risen (Lundeen, 1999).

The negative consequences of such standards (e.g. billions of dollar in added business expenses and the potential loss of thousands of telecommuting jobs) are not offset by OSHA's contention (unsupported by clear scientific evidence) that the regulations will save more than they will cost. Finally, the standards should not be applied to at-home offices because of the cost to personal privacy.

References

- Dorning, M. (2000). Home Workplace Rules Ignite Ire. *Chicago Tribune*.
<http://chicagotribune.com/news/printedition/article/0,2669,SAV-0001050145,FF.html>. Updated January 5, 2000. Accessed November 27, 2000.
- Gilroy, E. (2000). Statement Regarding OSHA's Withdrawal of Its Advisory on Home Offices. *National Coalition on Ergonomics*.
<http://www.ncergo.org/news.htm#homeregs>. Updated January 5, 2000. Accessed November 27, 2000.
- Hayworth, J. (2000). Hayworth, American People Claim Victory After OSHA Backs Off Telecommuter Regulations. *U.S. House of Representatives*.
http://www.veterans.house.gov/hayworth/press_releases/oshahom2.htm. Updated January 5, 2000. Accessed December 26, 2000.

- Koch, K. (2000). Home Offices Protected Under Workplace Rules; Employers Object. *CNN.com*. <http://www.cnn.com/2000/US/01/04/home.office/index.html>. Updated January 4, 2000. Accessed November 27, 2000.
- Lundeen, A. (1999). Repeated Trauma Injuries Down For Fourth Year. *National Coalition on Ergonomics*. <http://www.ncergo.org/news.htm#traumadownagain>. Updated December 16, 1999. Accessed November 27, 2000.
- Reuters. (2000). Workplace Safety Rules Cover Telecommuters-OSHA. *Reuters*. <http://www.phoenixlive.com/lucifer/pythias/Workplace%20Safety%20Rules%20Cover%20Telecommuters-OSHA.htm>. Updated January 4, 2000. Accessed November 27, 2000.
- Robins, J. (2000). Should Workplace Safety Standards Apply to Telecommuters. *SpeakOut.com*. <http://www.speakout.com/Issues/Briefs/1174/>. Updated February 17, 2000. Accessed November 27, 2000.
- Thibodeau, P. (2000, November 20). OSHA releases final rules for workplace ergonomics. *Computerworld*, 20.
- Trott, B. (2000, November 20). OSHA sets ergonomics ground rules as businesses object. *InfoWorld*, 24.