TUESDAY, FEBRUARY 15, 1994
4:00 - 5:30 p.m.

CONCURRENT SESSION TWO

Liability Issues Arising From Computer Misuse by Students, Faculty and Administrators

Faculty:

Howard Bell
Sally Harwood
LIABILITY ISSUES ARISING FROM COMPUTER MISUSE BY STUDENTS, FACULTY AND ADMINISTRATORS

PRESENTERS:

HOWARD W. BELL
VICE PRESIDENT FOR ADMINISTRATIVE SERVICES
UNIVERSITY OF CINCINNATI
CINCINNATI, OHIO

SALLY S. HARWOOD
ASSOCIATE GENERAL COUNSEL
MICHIGAN STATE UNIVERSITY
EAST LANSING, MICHIGAN

Presented by Stetson University
College of Law at the:

15th ANNUAL NATIONAL CONFERENCE ON LAW & HIGHER EDUCATION
Clearwater Beach, Florida
February 13-16, 1994
LIABILITY ISSUES ARISING FROM COMPUTER
MISUSE BY STUDENTS, FACULTY AND ADMINISTRATORS

Stetson University College of Law
The Fifteenth Annual National Conference on
Law and Higher Education: Issues in 1994
February 13-16, 1994

Howard W. Bell, Ph.D.
Vice President for Administrative Services
University of Cincinnati

Sally S. Harwood
Associate General Counsel
Michigan State University*

RESPONSIBILITIES AND LIABILITIES
IN COMPUTER COMMUNICATIONS AND RECORDS

I. ACCESS AND OWNERSHIP

A. Communication Developments. Concerns about misuse of networks
have kept pace with the building of the "information highway".

1. Network growth. In January, 1994, Vice President Gore
challenged communications executives to ". . . connect all of our
classrooms, all of our libraries, and all of our hospitals and
clinics by the year 2000."

2. Increased liability. Administrators' concerns of
unauthorized access or misuse of network access, and hacking, are
magnified by the knowledge that not only their institution, but
institutions and individuals around the world may be affected via
the campus network account. Increased vulnerability to misuse of

*The assistance of Paul M. Hunt, Ph.D., Vice Provost for Computing
and Technology at Michigan State University, is gratefully
acknowledged.
the internet has been attributed to the number of campus computers not under control of computing professionals. As Charles Bowman, associate director for computing services at the State University of New York at Stony Brook stated "Somebody in a laboratory figures there's nothing of interest in his machine and doesn't secure it properly, and that leaves a back door open for people to go anywhere in the world. You're now at the mercy of the weakest link in a security chain." "Gate Crashers: Campus computing officials are trying to crack down on ubiquitous 'hackers'", The Chronicle of Higher Education, October 20, 1993, pg. A23.

3. Health Care: liabilities for consequential damages. Computer network communications are now being used to transmit tests and scans and other images, as well as to connect doctors and patients in long-distance interactive diagnosis and treatment. Tort litigation is increasing for all types of computer activity, and medical misdiagnoses or incorrect treatment because of computer failures could result in extensive consequential damages. Developers and sellers of computer software, including educational institutions, must take care to limit damages by contract. "Faulty Software Means Business for Litigators", Wall Street Journal, January 21, 1994.

B. E-mail

1. Culture. Though electronic mail is rapidly becoming more widely used ("E-mail from Bill", New Yorker, Vol. LXIX, No. 45, January 10, 1994), the e-mail culture has not developed very clear expectations for proper use. There is a growing need to balance
such issues as personal privacy versus corporate proprietary rights, data transmission, and the way in which legal rules of evidence apply to information stored in computers. The handling of e-mail is a particularly gray area. "Constitutional Law in the Electronic Age", Management Review, Sept. 1992, pg. 24.

2. Back Up Copies. When is an e-mail message (or any electronic file) truly discarded? Users feel that when they hit "delete", a message is gone. Due to the existence of system back-up copies for use in case of crash restores, that is rarely true. Aside from the case of a subpoena, the question arises whether recourse to such back-up system images must be made to satisfy FOIA requests. (C.f., Kendall, M.A., "Access to Information Beyond Reach as Computer Tape Lengthens Bureaucratic Red Tape," Vol. 3, Software Law Journal, April 1990, pp. 775-791.)

3. Administrative Access to Copies. Considerable confusion exists over access to and ownership of electronic mail messages, arising in part from the use of institutional computer systems for sometimes very personal messages. May supervisors read employee e-mail messages, and if so under what circumstances? May misdirected messages be read?

a. H.R. 1900, S. 984, Privacy for Consumers and Workers Act has been referred to committee and public hearings have been held. The proposed Act would prohibit employers from electronically monitoring their workers except under certain conditions, to avoid abuses of "spying" in the workplace. S. 1735, Privacy Protection Act of 1993, would establish a Privacy
Protection Commission to make recommendations for regulatory and legislative action to ensure that technological advances do not infringe on personal and corporate privacy rights. (For background, see DeBenedictus, J., "E-mail Snoops: Reading Others' Computer Messages May Be Against The Law," Vol. 76, ABA Journal, Sept. 1990, p. 26(2).

b. In response to faculty outrage at review of a faculty member's e-mail (which verified extensive non-university use by the faculty member's spouse), a major research university adopted the access policy attached as Addendum 1. Michigan State University includes a procedure for administrative file access as part of its general computer use guidelines. Policies should include procedures for access to E-mail and other electronic files of deceased or incapacitated employees.

4. Public Access (FOIA). If a public university owns all of its staff e-mail messages, what are the FOIA implications? Is e-mail equivalent to phone calls or to memos and letters?

a. Misconceptions regarding Freedom of Information requests for electronic mail may also extend to voice mail and may in fact skew campus usage or investment patterns artificially between these complementary technologies. In some jurisdictions, a voice mail message may be subject to the same public scrutiny under FOIA as an electronic mail message. However, it is less likely to be retained at the originating end (as much e-mail is) or retained as long at the receiving end.
b. The University of Michigan currently is resisting a writer's FOIA request for e-mail of its administrators, contending that the e-mail is most comparable to telephone calls which are not recorded and available under FOIA. The University has stated that it as an institution also would be barred by the federal Electronic Communications Privacy Act from reading electronic mail on University systems, even in order to determine whether it relates to a University use. A lawsuit is pending against the University of Michigan to make other electronic materials available under FOIA. The Chronicle of Higher Education, January 26, 1994, pg. A28.

5. Federal Wiretapping; Clipper Chip.

a. The federal government is considering a standardized encryption scheme to allow authorities to access private information over public data networks when necessary. The FBI is concerned that unbreakable encryption is becoming available to individuals, thwarting its ability to wiretap certain communications, even with a proper warrant. Encryption is important to privacy, and the goal would be allow difficult codes to protect U.S. companies, while still escrowing the clipper chip so the government could access the communications. Communications of the ACM, September, 1993, Vol. 36, No. 9, pg. 15.

b. The government would have to obtain voluntary compliance with use of the "clipper" encryption chip or outlaw any non-standard encryption schemes. The Digital Encryption System (DES) is another possibility. Questions include possible harm to

6. **Limiting Use of Network.** The University of Texas has been sued because of its withdrawal of network access from a user sending personal political opinions around the world. Although the University has a uniform policy which does not allow any non-University use (see Appendix 2), the user claims his free speech rights were violated.

7. **Commercial Linkage.** Use of institutional, state or regional, and national networks to send e-mail to commercial vendors is often a problem. (See, for example, Ladd, C., "Contractors Tap in, DOD Reaches Out: Networking, Pentagon Style," *Vol. 10, Legal Times*, May 23, 1988, p.1, col. 4.) The propriety of such use may be assessed based on the rules and conditions imposed by the network.

C. **Data Access.**

1. **Technological Environmental Factors.** Modern computer operating systems provide different levels of file protection, with widely varying default settings. A typical multi-user operating system might permit a user to set different file access security switches for members of a defined affinity group, for system staff, and for the world at large. Some operating systems utilize a "permissions" perspective while others utilize an "exclusions" perspective to accomplish similar ends. Virtually every system sets access by each user category one way or the other by default,
leaving it to users to change either the defaults, the individual access settings, or both.

2. Questions Arising From System Diversity. May the absence of an exclusion be construed as the equivalent of an access permission, given the dichotomous nature of "exclusion/no exclusion" and "permission/no permission" within the technology? This becomes particularly tricky when (in a heterogeneous networked setting) one unsophisticated student user, working on a home machine with a permissions-based file system, accesses a remote system with an unfamiliar, exclusions-based file system. If access control defaults on a faculty workstation are set to "permitted" or "not excluded" and a student reads sensitive files (grades? letters of recommendation? exam questions?), is that act the equivalent of reading material negligently left posted on a public bulletin board, or of stealthily entering an office and perusing the contents of an unlocked filing cabinet?

3. Informational Privacy. The common law of torts recognizes "privacy" with respect to publication of names and private information, false portrayals of persons, intrusions into private places, and personal dignity. The term "informational privacy" was coined in light of rising concern in the last two decades with respect to collection, maintenance, use and dissemination of personal information not encompassed by the common law torts. See Trubow, George B. "Watching the Watchers: The Coordination of Federal Privacy Policy", *Software Law Journal*, Vol. III, pg. 396. Federal statutes and state Freedom of Information
Act cases reflect that information kept or disclosed in hard copy is less intrusive of informational privacy than information on computer disk or tape. The Privacy Act of 1974, 5 U.S.C. § 552a is administered by the federal Office of Management and Budget. Inadequacies of the Privacy Act in controlling the increasing linkages of information between federal agencies led to enactment of the Computer Matching and Privacy Protection Act of 1988, amending 5 U.S.C. § 552a.


a. Commercial software packages are available for maintaining student records, but rarely map directly and accurately to established distinctions between "directory" and confidential information. In addition, some may anticipate use of Social Security Numbers as student identifiers.

b. Students' FERPA rights to inspect their own records must be taken into consideration in the design and implementation of student information systems.

c. Advancing technology permits the annotation of electronic records with plain text comments. Inappropriate annotation by staff could represent a serious institutional embarrassment and potential liability. The monitoring of such annotation, or its prohibition, must be considered.
d. The ability to build automated decision making into new systems will ultimately impact staff data access predicated upon a "need to know" standard.

II. BULLETIN BOARDS

A. Communication Forum. Computer bulletin boards can be useful arenas for accessing information, news, and political commentary on a wide range of topics and can serve as forums for debate. *Nieman Reports*, Fall 1992, volume 46, number 3. Currently approximately 12 million Americans are linked together through a mesh of computer networks. The largest network, Internet, links over 1.7 million computers in more than 135 nations and is adding new users at the rate of 8% per month. Possibly the greatest impact of the rapidly growing worldwide computer networks is that they are allowing the formation of new communities of people who share common interests in real time. *USA Weekend*, January 21-23, 1994, pp. 4-6. However, the potential exists for abusive, antisocial messages and a vicious electronic lynch mob mentality, which may stem from the need for instant and fleeting fame or be a negative consequence of this medium, being one in which opinions can be posted namelessly. *Macworld*, March 1992, Volume 9, Number 3. (See Jansen, E.C., "An Electronic Soapbox: Computer Bulletin Boards and the First Amendment," Vol. 39, *Federal Communications Law Journal*, Oct. 1987, pp. 217-258.)

B. Free Speech. What can or should be censored? At the root of this question are liability issues for network and bulletin board operators for materials transmitted over their services.
1. Criminal Activities. According to the U.S. Customs Service, computerized bulletin boards are becoming increasingly popular conduits for child pornographers who use them to acquire subscribers to a worldwide pornographic picture ring, based in Denmark, charged its members around $80 per year and used computers and telephone lines to transmit explicit photos of children ages 5 to 12. *Time*, March 15, 1993, pg. 22.

2. Operator Liability. A case involving an instructor at the Santa Rosa Junior College in California has ignited a national debate over the liability of a bulletin board operator over the contents of his/her bulletin board. The instructor established a "Men Only" and "Women Only" service for students which resulted in two women filing sexual harassment suits. The instructor was suspended with pay pending an investigation. The instructor has pleaded innocence arguing that he is protected by freedom of speech and that his role as the system operator is comparable to that of a bookseller. *The Chronicle of Higher Education*, May 19, 1993, Vol. 39, No. 37, pg. A28.

3. Operator Censorship. A professor of microbiology and immunology at Northeastern Ohio University's College of Medicine was severely criticized by users of the Internet's Usenet when he activated a program he had written allowing him to cancel anonymous messages to a given discussion group that he considers unscientific or abusive. The professor was condemned for assuming the role of censor over the network and was viewed as setting a bad precedent that might be copied by others with disastrous results. The

4. Public School Access. A related problem arises from the growing number of networking alliances between universities and K-12 schools. Electronically published materials (e.g., in some of the "alt" newsgroups of USENET) of which most American university communities are tolerant or protective may raise scandal or legal complaints if accessed by minors within the K-12 system. Again, in light of advances in distributed processing it is erroneous to assume that an institution's central computer center will be the sole repository of relevant expertise, hardware, or activity.


C. Distance Learning.

a. TriState online (TSOL) provides a series of information services to Cincinnati residents through an electronic bulletin board. Included in the TSOL are library information services. Special Libraries, Spring 1992, volume 83, number 2.

b. Use to reach non-traditional students and augment learning of traditional students. Online Interactive Education (OLE) uses online computer communications to simplify and enhance course work outside of the traditional classroom setting. The
technology is designed to reduce classroom meetings by allowing students to submit assignments, communicate with instructors, pose questions or interact with other students while online.

i. Has been successfully tried at Northern Kentucky University, in Highlands Heights, Kentucky. Information from materials provided by CBD, Inc., A Cincinnati Bell Company.

ii. California Polytechnic State University has announced that it will partner with vendors and other colleges to develop multimedia courses that can be delivered on demand to far-flung students, including customizable classes delivered via an electronic network to corporate America. Computerworld, January 17, 1994, pg. 70.

D. Institutional Role.


2. Difficulties in Proof. Bringing charges against suspected electronic misconduct poses special challenges. Network logging mechanisms can provide high quality evidence of the timing
of and locale from which break-ins are attempted, hate mail sent, etc. What they do not provide is positive identification of the person who was using the keyboard. Eye-witness identification is unlikely, and sign-in protocols are undermined by trips to the printer, calls of nature, etc. Coupled with the tendency of campus judiciaries to utilize high standards of proof in serious disciplinary cases, doubts surrounding the identity of perpetrators may result in dismissed charges. This in turn may focus administrative attention on possession of "cracking tools" (software designed to circumvent security) as the evidence of choice in establishing misbehavior. This raises immediate questions regarding the privacy of personal files, in so much as the tell-tale software will only be detected by official inspection of files the confidentiality of which normally would enjoy official protection. Importation of such technical concepts as probable cause or fruit of the poisoned tree into computer lab operations and student judicial proceedings will not be welcomed by many educators.

E. Violation of Professional Ethics

1. Practicing Law. Bulletin boards, like Prodigy's legal bulletin board, can be used by an attorney who posts advice in much the same way as an attorney who writes a syndicated column on the law. However, because the attorney, via the bulletin board, has the ability to engage in a dialogue with those who pose the questions an attorney-client relationship can be created. This practice poses at least two potential problems: 1) If the client
is in a state in which the attorney is not licensed he/she could be guilty of engaging in an unauthorized practice of law, a crime in many states; 2) the advice given is not always complete. ABA Journal, June 1993, Vol. 79, pg. 36.


III. CRIMINAL PENALTIES RELATING TO COMPUTER COMMUNICATIONS.

Increasingly, educational institutions are taking a tougher attitude against hackers and unauthorized access, turning more often to criminal charges instead of purely internal sanctions. Institutions where access was obtained may call authorities routinely to avoid possible lawsuits from other entities which may have been harmed. "Gate Crashers", supra. Charges may be based on a number of the following criminal statutes.


1. Proscribes the interstate transportation of stolen "good, wares, merchandise, securities or money, of the value of $5,000 or more". 1992 amendments to title 18, § 2319, penalize knowing distribution of infringing copies, contrary to some earlier caselaw. Dowling v. U.S., 473 U.S. 207, 105 S.Ct. 3127, 87 L.Ed.2d 152, on rem. 789 F.2d 1314 (1985).
2. Dowling distinguished in U.S. v. Riggs, 739 F. Supp. 414 (N.D. Ill., E.D. 1990), holding that proprietary "trade secret" information in telephone company computer text file was "goods, wares, or merchandise" per § 2314, without respect to copyright interests, and that the federal Computer Fraud and Abuse Act was not intended to be exclusive.

*a/k/a Prophet; codefendant Neidorf, a/k/a Knight Li


1. Proscribes use of wire communications in furtherance of a scheme to defraud. United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978)(defendant obtained source code of federal computer through unauthorized telephone access to computer; conviction upheld).

2. Use of an interstate computer data network to transfer stolen computer files meets the wire communication element of the offense. U.S. v. Riggs, supra.

C. State Statutes. Nearly all states now have statutes specifically dealing with computer abuse. National Center for Computer Crime Data, cited in Hansen, supra, at 728 n. 35. For a state-by-state summary, see Bender, supra, at 4B.15[2].

1. Scope. Some concern only situations in which access is unauthorized, while others proscribe unauthorized use even though access may have been authorized. Other variations relate to the purpose of unauthorized access ("fun" or profit?) and its effect of disruption or destruction.

3. Example. The California statute (Cal. Penal Code § 502) is the most comprehensive.


2. Encompasses a variety of offenses, dealing with access to U.S. government computers or information affecting national security or financial institution records; also prohibits trafficking in passwords with intent to defraud, with an effect on interstate commerce (the primary Morris indictment) or government interests.

3. Attempts to commit offenses are also offenses.


5. Jurisdictional shortcomings: Does not address federal/state jurisdictional questions, provide for broad interstate prosecution or provide for civil remedies for victims.

6. Substantive shortcomings. Unless trafficking in passwords can be shown, requires "knowing" access to federal computers, which could be difficult to show in the case of a virus, since the
programmer has no control over what computers will be infected by the virus. Some types of viruses could be started without unauthorized access, with innocent later users spreading the virus.

7. Penalties. As provided 18 U.S.C. 3623. (Fine, up to ten years imprisonment, or both, for first conviction; fine and up to twenty years for repeat offense.)


F. Title III, Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 et seq. While not specifically dealing with "computer crime", portions of Title III controlling interception of communications without permission may be relevant to any case relying on computer spy functions for detection of unauthorized access and activity.

G. Limits on Application. Strict construction of criminal statutes limits application in the event of any ambiguity. New York v. Weg, 450 N.Y.S.2d 957 (Crim. Ct. Kings Co. 1982) (construed statute prohibiting unauthorized control over equipment of another for personal gain as applying only to equipment for hire to the public, not to internal office equipment such as computers), Dowling v. United States, supra. (statement of construction role for federal criminal statutes).
H. Update of Other Criminal Laws. Since criminal laws are strictly construed, statutes may need to be amended to include computer variations of traditional crimes. For example, 18 U.S.C. §§ 2252(a) and 2256 were amended specifically to proscribe computer transmission of material sexually exploiting children.

I. Trespass. To what extent are hackers guilty of trespass but not guilty of criminal intent? The Electronic Frontier Foundation formed by Mitch Kapor, of Lotus 1-2-3 and John Perry Barlow, Grateful Dead lyricist, intends to lobby for laws that encourage the use of public networks and incorporate a distinction between trespass and criminal intent. Forbes, January 7, 1991, Volume 147, Number 1.

INTELLECTUAL PROPERTY PROTECTION AND INFRINGEMENT

With respect to commercialization of computer software, the formerly prevalent "computer culture" of general sharing of new developments is undergoing a change to a more controlled and limited grant of rights. Discussions and hearings have been taking place concerning how to disseminate intellectual property on computer networks without relinquishing the rights of its owners. "Computers and Copyrights", The Chronicle of Higher Education, November 24, 1993, pg. A15; "Remaking Scholarly Publishing", The Chronicle of Higher Education, December 15, 1993, pg. A15. Meanwhile, copyright and patent owners are becoming more aggressive in protecting their intellectual property rights.
I. MULTIMEDIA

A. What is multimedia and what is its impact?

1. **Description.** The term multimedia is amorphous. And while the term is not fixed it is clear that multimedia works combine text, images, sound, computer software and associated computer hardware. Multimedia works bring together two entirely different areas of the law, entertainment and computer law. Hence, it is best that anyone considering advising multimedia clients be versed in both computer and entertainment fields and the relevant issues in both. "Interactive multimedia: what is it, why is it important and what do I need to know about it?" *Computer-Law Journal*, December 1992, Pgs. 585-596.

2. **Effect on Legal Practice.** Multimedia, the combining of audio and video on a desktop computer, will impact the practice of law in many ways within the next 10 years. Multimedia will enable attorneys to enhance their documents with both audio and video components, change an attorneys' interactions with the courts with paper briefs falling into disfavor, and change the way attorneys do research. The authentication of evidence will also change given the ease whereby digital documents can be altered without a trace that the data was ever manipulated. *ABA Journal*, August 1993, 79, Pg. 52 (4).

3. **Characteristics.** Information technology has the power to transform human institutions and the relationship between people and machines. Currently in the area of computer as teacher, most of the human characteristics attributed to the computer, patience,
even-temper, and always attentive to the needs of individuals, are commonly associated with females. Currently there are trends, worldwide, to define more and more women in the third-world, and women of color, and working-class women as "wetware" while middle-class white women become more highly paid "computer peripherals". Wetware is defined as "biological material essential for the operation of the machines". The reference to "computer peripherals" refers to the use of "computer-based artificially intelligent expert systems" that limit a worker's ability "to speak or act from her or his own expertise" making them "comparable to a modem, a printer, or other 'computer peripheral'". Feminist Teacher, Winter 1992, Volume 6, Number 2, Pg. 16 (5).

B. Issues involved with producing multimedia works.

1. Widespread Copyright Violations. Virtually anyone today can use scanners, sound boards and multimedia authoring systems to incorporate copyrighted material into a business presentation or other microcomputer production. Unfortunately, most such uses are technically illegal. Vendors should make it easier to comply with the law by negotiating all-rights buy-outs with the creators of material and passing along royalty-free status to the buyers of their products thereby reducing the current rampant copyright abuse among multimedia users. PC Magazine, February 23, 1993, Volume 12, Number 4, Pg. 99 (2).

2. Production needs. There are a series of legal do's and don'ts involved in the production of interactive technology. Among the legal do's are: 1) DO it in writing; DO acquire ownership of
the elements contained in the production; DO look for rights that must be licensed; DO due diligence (to include if necessary, obtaining a copyright chain of title); DO look out for real people (and the possibility of defamation or invasion of privacy issues). Among the legal don'ts are: DON'T paint yourself into a rights corner (always have alternatives to the work you want to license); DON'T assume a work is public domain; and DON'T copy (the legal prohibition against sound-alike and look-alikes is expanding). "The legal do's and don'ts of producing for interactive technology." Billboard, August 7, 1993, Pg. II4(1)

3. Photography. Publishers of electronic books, photographs, and art collections on CD-ROMS are finding that it is not always easy to get licenses to copyrighted material from the authors and artists who own them. A number of photographers are trying to flesh out a new set of copyright arrangements for photographs that take into account not just the number of copies of an image but the manner in which the images are used. These rights, called service rights, have been licensed in the music recording industry for years. A company, the Electric Book Company, was recently started to become a sort of photographic ASCAP, with the mission of becoming a domestic and international licensing agent between photographers and CD-ROM publishers. InfoWorld, March 9, 1992, Volume 14, Number 10, Pg. 670 (1).

4. Variety of rights. With multimedia works copyrights constitute an area of primary concern because the great bulk of multimedia works involve textual, audiovisual and sound recordings, and other artistic works that have been historically protected by
copyright. However, patents and trademarks may apply as well. (See below.) In producing multimedia works one must deal with the special issues associated with "Pre-existing works", "Literary works", "Moral rights", and "Trademark rights". "Multimedia Works Require Broad Protection" The National Law Journal, November 1, 1993, Volume 16, Number 9, Pg. 611, Column 1 (69 col in).

5. Licenses. The types of licenses required for music in a multimedia production will depend on whether the multimedia show is used for "private performances" or for public presentations. The types of licenses required will depend on a variety of issues involving how the music is integrated into the multimedia work. For example, if the presentation includes video, animation, or other forms of movement, and the music is synchronized, one may need a synchronization license to copy, a performance license, and a videogram license to perform. In general, with many multimedia productions one may need more than one license. InfoWorld, November 9, 1992, Volume 14, Number 45, Pg. 28 (1).

C. Ethical dilemmas in using multimedia technology.

1. Codes. While professionals in a variety of fields from lawyers to physicians have adopted ethical codes professionals in the information technology field have no agreed code of conduct. Currently in the US, there are four organizations promoting four different codes of conduct. While some of the behavioral precepts are similar, others are not. Journal of Business Ethics, September 1993, Volume 12, Number 9, Pg. 709 (18).

2. Attitudes. A survey of the ethical beliefs of experts and high technology students in computer-related situations
concluded that the various groups of students disagreed significantly on eight out of nineteen ethical problems. Journal of Business Ethics, May 1993, Volume 12, Number 5, Pg. 359 (12).

D. Multi-media patents.

1. Compton's. Compton's NewMedia was awarded patent number 5,214,671 in August, 1993, covering the retrieval of multiple types of data from a single source. The core multimedia technology upon which it is based already is used in thousands of multimedia applications. The patent covers the retrieval of photo, audio, text and video data from multimedia databases. Compton's plans to collect royalties on the sales of search-and-storage methods used with interactive television, as well as on competing CD-ROM applications. Some legal experts contend that Compton's patent does not cover as broad an area as the company believes. Computerworld, November 22, 1993, Vol. 27, No. 47, pg. 28.

2. Tektronix. The patent claimed by Tektronix is on software that uses indexes to display video images. Tektronix has contacted vendors to request licensing discussions. "Tektronix's claim to patent surprises multimedia vendors", Infoworld, March 1, 1993, Vol. 15, No. 9, pg. 10.

3. Prior use. Microsoft, Apple Computer (Hypercard) and others have used multimedia concepts and displayed products before Compton's developed its multimedia, and its claim is an emotional issue for the computer software industry.

4. Academic materials. Educators have used multi-media in a general sense for many years and now are increasingly involved in
developing computer versions, often without any concept that these may violate any patents.

II. SOFTWARE COPYRIGHT PROTECTION.

A. Statutes.


2. Fair Use. In addition to the general fair use exception, 17 U.S.C. § 117 limits the exclusive rights otherwise granted a copyright owner by excepting certain activities of an owner of a copy of the work from the § 106 proscription against infringement:
   a. Making a copy of or adapting a program "as an essential step in the utilization of the computer program in conjunction with a machine";
   b. Making a copy of or adapting a program "for archival purposes only".

3. Applicability of Limits to State, 17 U.S.C. § 511 (added by Copyright Remedy Clarification Act, P.L. 101-553, effective November 15, 1990). Provides very specifically that "any State, any instrumentality of a State, and an officer or employee of a State or instrumentality of a State acting in his or her official capacity" will not have Eleventh Amendment or any other sovereign immunity from copyright infringement suits.

B. Illegal Copies. Violations of copyright laws through the distribution of illegally copied software can and are creating problems.

1. Distribution. In mid 1992, the FBI closed down the Davy Jones Locker service in Millbury, MA, an electronic bulletin board
that was allegedly distributing illegally copied software. 


2. Criminal. In June 1992, the U.S. Senate passed a bill making the illegal distribution of copyrighted software a felony. 


3. Network tools. The advent of multi-institutional database resources (such as GOPHER, WAIS, etc.) deserves attention. These powerful tools are easily available following a brief period of apparently exponential growth in popularity. Their utility in research, instruction, and service outreach is clearly great. At the same time, the software necessary for international publication of data, music, and images -- potentially in pirated or impermissibly altered forms -- is sufficiently simple to permit an advanced undergraduate to embroil an institution in difficulties from her or his desktop, using an inexpensive workstation. For example, a law-abiding computer scientist may not know much about royalty payments to musical composers. The fact that the university marching band performs a selection in the stadium may not in itself suffice to permit a digitized recording of the performance to be made available to the world via GOPHER over the Internet. Institutions must confront the fact that the technology to do so is now widespread.

C. Protection of New Technology. The possibility of copyright protection for virtual works, virtual objects and virtual realities is discussed in Russo, J. and Risch, M., "New frontiers (copyright issues with virtual reality", The National Law Journal, Oct. 12,
1992 (finds a "general consensus" that such works merit copyright protection).

D. Ownership.

1. Work for hire. 17 U.S.C. § 101 provides that the copyright in works for hire vests in the hiring party. A work for hire is a work product of an employee or a particular type of work product of an independent contractor pursuant to a written agreement identifying it as a work for hire. Community for Creative Non-Violence v. Reid, 109 S. Ct. 2166 (1989) mandates use of common law agency rules to determine whether a hired party is an employee or an independent contractor.

2. Joint works. The copyright to a joint work is owned by all co-authors whose contribution, alone, would have been entitled to copyright protection. A hiring party does not become a co-author by describing to the contractor what is to be done, even if the instructions are fairly specific. S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081 (9th Cir. 1989).

3. Need to Clarify at Outset. The higher education environment encompasses many situations in which the employment status of the creator of or contributor to a software program may be ambiguous. For example, a student paid by the university to assist in laboratory course sessions develops, at the request of the professor but at home without direction, a program for use in the course. The primary rule, forgotten in too many cases where a "reasonable" assumption of ownership is made, is to document the ownership when any doubt exists.
E. Joint Research. Computer companies are active in sponsoring university research, through gifts of equipment and software as well as grant funding. As with other research, computer research planned in conjunction with a group of commercial funding ventures should be disclosed in a filing under the National Cooperative Research Act of 1984 (15 U.S.C. 4301, et seq. to help limit antitrust liability.

F. Defenses to Copyright Infringement Claims.

1. Fair Use. 17 U.S.C. § 117; Parties Covered by Exceptions. Although § 117 exceptions extend only to owners of a copy of a copyrighted program, contrary to the CONTU Report recommendation to extend exceptions to "rightful possessors" (see SOS, Inc. v. Payday, Inc., supra), recent cases imply that shrink-wrap licensees, if not all licensees, will be considered covered by the exceptions. Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255 (5th Cir. 1988); Foresight Resources Corp. v. Pfortmiler, 719 F. Supp. 1006 (D.Kan. 1989).

2. 17 U.S.C. § 117; Right to Adapt Copy. Adaptation of a copy may be necessary to make a program compatible with the copy owner's hardware, and Midway Mfg. Co. v. Strohon, 564 F. Supp. 741 (N.D. Ill. 1983) would limit the adaptation right to that situation. A broader interpretation is given in Foresight Resources Corp. v. Pfortmiler, supra, though the court did forbid sale of the enhanced copy by the copy owner/adaptor.

3. 17 U.S.C. § 117; Right to Load Copies. The first exception under § 117 has been interpreted to allow only a copy owner/user to load his copy into his own computer memory

4. 17 U.S.C. § 117; Archival Copies. Some cases limit of the archival copy exception to situations in which the copy owner was avoiding damage from "mechanical or electrical failure" rather than from dangers faced by any type of physical copy. (See e.g. Micro-Sparc, Inc. v. Amtypre Corp., 592 F. Supp. 33 (D. Mass. 1984)). As with respect to other § 117 exceptions, Vault Corp. v. Quaid Software, Ltd., supra, takes a broader view of the archival exception.

5. Copyright Misuse. A developing defense to infringement claims is the assertion that the copyright holder misused the copyright, as for example by antitrust violations, and is not entitled to protection. United States v. Loew's, Inc., 371 U.S. 38 (1962). Because the defense is a court-created equitable doctrine, it is subject to the "clean hands" doctrine. Atari Games Corp. v. Nintendo of America Inc., supra at 845-846.

III. PATENT PROTECTION.

A. Scope. Patentable subject matter includes any process, apparatus, or composition, or improvement thereof, which is new, useful and unobvious to persons of ordinary skill in the art. (35 U.S.C. 101).

B. Development. Past computer software patents have primarily concerned process control, but in recent years more deal with
user/computer interfaces. **Bender, supra,** at § 3A.07[3][b]. In general, applications for software patents have greatly increased in each of the last ten years, and commentators suggest that the 1990s will be the decade of patent litigation, as the 1980s was for copyright litigation. Stapleton, "Algorithm and Software Patents: Protection or Peril for the Industry?", *Supercomputing Review*, January 1991, pg. 35; **Bender, supra.**

C. See above discussion of multimedia patents.

IV. COMPLIANCE WITH THIRD-PARTY AGREEMENTS


1. **Servers.** The use of site licensed software on servers requires special attention. Some packages now offer technical implementations that limit simultaneous use to an authorized number of program images, e.g. "Framemaker" by Frame. As a rule, the less sophisticated a software package (or supplier) is, the more susceptible to improper use or exploitation via servers it will be. On the other hand, hardware manufacturers are actively selling campuses combinations of servers and diskless workstations that preclude the mid-80's model of "one stand-alone software copy per seat," e.g. LOTUS.

2. **Student Access.** Many software packages are initially designed for use in non-educational institutions. Their software licenses frequently restrict use, access to source code, access to documentation, etc., to "employees." Higher education institutions
frequently must negotiate amendments to license agreements to ensure appropriate access by students.

3. **Site Definition.** Many universities are responding to higher education leadership trends emphasizing "service outreach" to meet societal needs across diverse communities. To support this effort, computing units must provide remote access to information resources (such as application software and electronic databases) to employees (e.g., Cooperative Extension Service agents) and students in the field and to "non-traditional" or "distance" learners who are neither employees nor traditionally enrolled students. Moreover, with the rise of computer networks (NSFNET, NREN, their regional and state tributaries, and local "dial-up" access points supporting work from home) the entire concept of "site" (or "campus") loses utility.

4. **Reports to Vendors.** Many site licenses require periodic reports of new applications developed using the vendor's code, copies made for local distribution or sale, etc. In extreme cases, vendors may seek to require the names and addresses of all students who use their software, ostensibly to facilitate employers' searches for qualified or experienced tool users.

5. **Citizenship Restriction.** Some site or institutional licenses stipulate that access by some or all non-U.S. citizens must be restricted or prohibited. (Such software may not be clearly defense-related; one example is a large accounting management information system that has been offered as a donation to universities by a major consulting firm.) Legal or
institutional policies may preclude denying foreign students access to educational experiences or tools.


1. For Employees (including student employees)

a. Data processing operations, which are typically staffed by non-academic personnel, generally should establish codes of professional conduct for their employees. Use of tenure revocation procedures against faculty guilty of improprieties involving software license violations may be analogized with the use of such procedures for serious property crimes, but must be considered politically very difficult at best.

b. Many software packages stipulate that universities require all employees with access to a software package to sign non-disclosure agreements. This may pose special problems as an extra-contractual condition of employment for members of collective bargaining groups.

2. For Students (who are not also employees)

a. An institutional obligation to inform students of restrictions applicable to the use of institutionally supplied software must be recognized. Prior to the rise of server-based
software, a frequent technique was to include an acknowledgment of responsibility on sign-out forms with which students gained physical access to software. In a networked environment with literally hundreds of different packages (with different rules) available on-line, signed acknowledgments which give access to workstation seats are possible, but must be viewed as distant and abstracted in their implications for most students.

b. Students who use illicit software copies provided by faculty pose special problems. Are they to be treated as willing recipients of stolen property or as victims of grade-enforced coercion?

C. Secondary Intellectual Property Rights

1. Vendor Rights in Derived Code. A license for software which is itself a platform for the development of new software may reserve to the vendor various notice, use, or royalty rights concerning the derived code. Example: several very popular artificial intelligence or expert system generation packages are accompanied by such license provisions. Besides the distribution of potential royalty income, the assignment of potential liability for errors in the encapsulated expertise deserves consideration in such cases. (See Cole, G.S., "Tort liability for artificial intelligence and expert systems," Vol. 10, Computer-Law Journal, April 1990, pp.127-231.) In some cases, equipment "donations" may carry provisions concerning secondary intellectual property rights. Ensuring internal compliance monitoring can be a nightmare, particularly since high cost (e.g., $25,000 per workstation for

32
some artificial intelligence packages) makes shared use by many research groups likely.

2. **Notice to Users.** Institutions that provide faculty or students class or research access to software platforms or donated hardware with secondary property rights reserved to the vendor should provide timely notice that potential intellectual property rights accruing to the faculty or students from their efforts are encumbered.
3. The Faculty adopt the following policy and procedures to govern access to electronic files controlled by faculty and staff:

POLICY AND PROCEDURES
GOVERNING ACCESS TO ELECTRONIC FILES

PRINCIPLES:
The procedures are based on three fundamental principles:
1. Intrusion into electronic files requires carefully considered cause;
2. Controllers of files should be notified before accessing their files; and
3. The University has an obligation to protect the integrity of the University, its services, its confidential data, and the rights and property of the State.

DEFINITIONS
As used in these procedures:

1. "Electronic File" encompasses information stored and/or transmitted in electronic form, including but not limited to text, data, sound, graphics, images, and video, irrespective of its recording and transmission media or its format.
   Examples of electronic files include e-mail messages, databases, and magnetic tape files and subsets thereof.

2. "Controller of a file" is defined as follows:
   a. on a single user computer under the control of a single person (e.g., a computer in a faculty office) the files normally are controlled by that person;
   b. on computers accessed by more than one individual, but which do not have an operating system that identifies files with a specific user, the individual responsible to the University for control of the computer (e.g., the laboratory director or department chair) is considered to be the controller of electronic files resident on that computer;
   c. On multiuser systems, an individual is typically registered or given an account. The registered user or account holder is normally considered to be the controller of files held in that account;
   d. In "work for hire" situations where one party enters or edits material for the originator of a file, the one responsible for originating the material in the file is the controller of the file. The person charged with entering the material is usually considered to be an authorized user. For example, when a secretary or a research assistant working under explicit directions uses a computer to enter and edit a document for a faculty member, the faculty member is the controller of the file and the secretary or research assistant is an authorized user.

3. "Authorized User" includes the controller of a file and someone who is given explicit access to the file by a controller.

4. "System Administrator" is an individual who has been charged by a University unit with maintaining a computer system and its software at an acceptable level of performance for the service that it is expected to provide.

(continued)
POLICIES AND PROCEDURES GOVERNING ACCESS TO ELECTRONIC FILES
September 13, 1991

INTRODUCTION

The Electronic Data Advisory Committee was created by the University Committee to clarify the privacy and confidentiality status of electronic data and to draft procedures for the University to follow in accessing the information in this form.

The faculty and staff of the University should be under no delusions as to the essential confidentiality of their electronic files. Even when one takes elaborate precautions (e.g., file encryption) the nature of modern communication networks is such that true confidentiality is impossible to guarantee. In addition, the open records law may require public disclosure of electronic data. All users of these services should be apprised of these facts.

The Federal Electronic Communications Privacy Act of 1986 (18 U.S.C. sec. 2511) and parallel language adopted by allows the University to examine electronic information when necessary to protect the rights and property of the University. The proposed procedures provide a mechanism for doing so in a way that respects the rights of individuals involved.

The report that follows deals with the question of appropriate procedures for the University to follow in cases of requests for access to electronic files initiated internally. (Requests for access that originate external to the University will normally arise under circumstances described in Section 6 of these procedures. In such cases, the University will provide notice to the controller and the opportunity to respond, whenever possible.)

In general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to

1. meet the requirements of the state open records law and other statutory or regulatory requirements;
2. protect the integrity of the University and the rights and property of the State;
3. allow system administrators to perform routine maintenance and respond to emergency situations such as combating "viruses" and the like; and
4. protect the rights of individuals working in collaborative situations where information and files are shared.

Accordingly, the Ad Hoc Electronic Data Advisory Committee recommends the following actions:

1. The University should make a special and periodic effort to notify users that:
   a. Faculty Policies and Procedures include rules governing the privacy of electronic data;
   b. State or federal regulations may supersede these policies and procedures; and
   c. electronic communications and data files are not secure from unauthorized access;

2. Because the proposed policy does not address how departments and schools may access students' instructional accounts, departments and schools should codify their procedures for managing and gaining access to such accounts;

(continued)
PROCEDURES

1. Except as provided for in Sections 5 and 6, no one but an authorized user of an electronic file may intentionally access that file without receiving either
   a. The permission of the controller of the file; or
   b. The express written permission of the Vice Chancellor for Academic Affairs and Provost, who may grant such permission only in accordance with the procedures established by Sections 2 and 3 below.

2. Except as provided for in Sections 5 and 6, the Vice Chancellor for Academic Affairs and Provost may grant permission to those persons listed in section 2(b) to access a computer or electronic file only upon determining that the all of the following steps have been taken:
   a. The Vice Chancellor for Academic Affairs and Provost has received in writing a request for access that specifies the reasons for the requested access and lists the requested file(s) by name, contents, or a description that clearly limits access to the file(s) necessary to further the purposes designated in Section 2(f).
   b. The written request has been made by a dean, director, department chair, vice-chancellor, or other person who has responsibility for protecting the integrity of the University, its services, and the rights and property of the State.
   c. The Vice Chancellor for Academic Affairs and Provost has notified in writing the controller of the file(s) that a request for access to the specified file(s) has been made and is pending. When there is doubt as to who is the controller of a file, notice should be sent to all the known individuals likely to have such an interest.

   Notification must, at a minimum,
   i. specify the name of the party requesting the file(s);
   ii. list by name, description, or contents the file(s) requested;
   iii. indicate that unless waived in writing by the controller of the file(s) within four days of notification, an inquiry as specified in section 2(d) of these procedures will be held to examine whether justification exists for granting the requested access;
   iv. indicate that in the event a section 2(d) committee has been appointed, the controller of the file(s) has a right to make known to the committee his or her views on whether access is justified;
   v. indicate that the file(s) in question shall not be altered or deleted by anyone, including the controller and that alterations or deletions may be a basis for disciplinary action; and,
   vi. if relevant, indicate that the Vice Chancellor for Academic Affairs and Provost has exercised his or her power under section 3 to take the minimum steps necessary to preserve the contents of the subject file(s).

   d. The Vice Chancellor for Academic Affairs and Provost has appointed a committee of three members, all of whom are otherwise uninvolved in the request and at least two of whom are members of the faculty or academic staff (as is appropriate to the case), to inquire into whether a justification under section 2(f) exists to warrant granting the requested access. Unless granted additional time, the committee will conduct its inquiry and make a written report to the Vice Chancellor within ten calendar days of its appointment.

   (continued)
PROCEDURES

At a minimum, the committee shall

i. examine the written request for access provided to the Vice Chancellor and Provost under Section 2(a); and

ii. offer all those notified under Section 2(c) an opportunity to make known to the ad hoc committee their views on whether access is justified.

e. The Vice Chancellor for Academic Affairs and Provost has received the results of the inquiry specified in Section 2(d) of these procedures or has received the controller's waiver of the section 2(d) inquiry.

f. The Vice Chancellor for Academic Affairs and Provost finds that the requested access is necessary to protect the integrity of the University, its services, and the rights and property of the State.

g. The Vice Chancellor for Academic Affairs and Provost has put in writing, with as much specificity as possible, the reasons for granting access to the file(s).

3. Upon the written request of one of those persons listed in section 2(b) or on his or her own initiative, the Vice Chancellor for Academic Affairs and Provost may authorize the appropriate University unit to take all necessary steps to preserve and save the contents of any file(s) within the University's computer systems. An order to preserve the contents of the file is meant to assure that the data in the file(s) is not destroyed, altered, or lost. Any such order does not constitute permission to open, read, or otherwise use the contents of the file(s). Access to the contents of the file(s) shall be obtained only under procedures specified herein or under conditions stated in Sections 5 and 6.

4. All requests for access to electronic files made under the open records law shall be made through the office of the University's Custodian of Records. It is recommended that the office of the Custodian of Records promulgate procedures consistent with the open records law and the principles expressed in these procedures. Such procedures shall provide for notice to the controller before public disclosure, whenever possible.

5. Nothing in these procedures is meant

a. to supersede the usual procedures followed by departments and schools in monitoring student accounts given for specific course work; or

b. to preclude computer system administrators from authorizing the routine maintenance of campus computer or communication systems or the rectification of emergency situations that threaten the integrity of campus computer or communication systems, provided that use of accessed files is limited solely to maintaining or safeguarding the system (which may include safeguarding the system from illegal use) or solving specific problems.

6. Nothing in these procedures is meant to either limit or expand access to files pursuant to or United States statutes or regulations, such as those governing patient records, student information files, open records, criminal investigations conducted by federal, state or local law enforcement authorities or certain personnel actions.
YOU MUST READ THE FOLLOWING STATEMENT BEFORE USING THIS ACCOUNT:

By using the account referenced above, I acknowledge that the use of accounts is governed by Policies for Use of Computer Accounts (available in the Jönsson Mainframe Center 2nd level, McDermott Microcomputer Center 3rd level, UTD Bookstore, and MP3.204).

In particular, I agree that computing facilities will be used only for instructional activities directly associated with the University of Texas at Dallas, that software licensed to the University will not be copied unless permission is granted in writing, that only information necessary and appropriate for my role at UTD will be accessed and will be used solely for that purpose, and that the account will be used ONLY by the person whose name (see User Name) appears above. This policy is effective and binding the first time this person logs in using the Account Name (Userid) referenced above.
**Policies for Use of Computer Accounts**

Computing resources have substantial monetary value. In order to retain integrity in the use of UTD's resources, and to minimize the possibility of loss to us all through security breaches, the following policies and procedures should be observed in the use of all academic computing resources. Failure to adhere to these policies and procedures and applicable State/Federal law may result in the termination of your privilege to use UTD computing facilities, irrespective of its consequence, and/or other disciplinary action including criminal prosecution.

* Facilities, including electronic mail, can be used only for instructional, research, and administrative support activities directly associated with and administered through The University of Texas at Dallas.
* An authorization is issued to one individual, it may be used only by that person, or the faculty sponsor, and may not be transferred, temporarily or permanently. The person to whom the authorization is issued is responsible for the safekeeping and legitimate use of the authorization, including protection of any password.
* Accounts may be used only to access machines for which a priori authorization has been granted and to access or process only information appropriate for the user's role at UTD.
* The ACC adheres to the guidelines laid down by EDUCOM in *Using Software—A Guide to the Ethical and Legal Use of Software for Members of the Academic Community*, copies of which can be obtained in MultiPurpose 3.204.

**STUDENT INSTRUCTIONAL ACCOUNTS:**

* Student instructional accounts are issued upon payment for the current semester of the Academic Computer Resource Fee of $45 per student; this covers the use in all UTD classes of all standard instructional computing resources; students not using university computing resources are not required to pay this fee; a surcharge of $10.00 is due when, at any time during the semester, the amount of expendables (such as paper) and/or disk space usage exceeds the base allocation;
* Standard instructional computing resources currently comprise those available within the student labs in the McDermott Microcomputing Center, those available from a student instructional account on the IBM 4381 mainframe, and those available on the CSCLASS and APACHE UNIX file servers.
* Student instructional accounts may be issued to the following persons: students currently registered at UTD; former UTD students during the semester immediately following graduation; students currently registered at other UT system institutions; as a courtesy to students currently registered at other institutions when requested by an official of that institution and approved by the UTD Director of Academic Computing.
* Payment of the fee may be made at registration or at the Bursar's Office; user accounts on the IBM mainframe and UNIX systems are issued at the Jonsson facility upon production of fee receipt, which is also required for the Microcomputer Center. Students may visit the Microcomputer Center three times before obtaining an account.
* Accounts may only be used for work associated with classes in which the student is currently registered (or for which an 'incomplete' grade had previously been assigned) or for other activities directly associated with UTD; use is permitted through the day final grades are due; a specific UserID from the previous semester can be reactivated, if requested, and associated files will be available to be restored.
* Use of specialized research facilities requires an instructor's request, permission of the organization owning the equipment, and submission of an Academic Computer Account Request form.

**FACULTY AUTHORIZED ACCOUNTS:**

* Other than student instructional accounts and external accounts, all other accounts must be sponsored by a current UTD faculty member or administrative department head using the Academic Computer Account Request Form; this form is obtained by calling 2651 and should be returned to the ACC (M/S JO21 or Room MP3.204);
Thesis/dissertation accounts may only be issued to students currently enrolled in dissertation or thesis courses; the faculty sponsor should be the student's advisor; use is permitted through the day preceding the first day of classes for the following semester, otherwise the same conditions apply as for class accounts including payment of the Computer Resource fee.

Course TA accounts are issued for the support of instructional use of computing facilities and are valid only for the semester in which they are issued.

Research accounts are issued to the sponsoring faculty member and may be used by that faculty member, or they may be assigned to another person if that person's name is identified on the account request and they are an employee (TA, RA, research scientist, etc.) of UTD; the faculty member is responsible for the account which may be used for research purposes only; accounts are reviewed annually and they remain active as long as they are in use, the faculty member to whom they are issued is on the faculty, and if assigned to another person, that person remains a UTD employee.

Administrative support accounts are for use by UTD employees other than faculty, and students.

With the exception of thesis/dissertation accounts for which the student pays the Academic Computer Resource fee, all other accounts are directly billed for consumables such as paper, and for disk space usage above base allocations. Hence, a valid UTD Fund/Org Number must be provided, with authorized signature, when the account is requested; other resources, such as computer time, are tracked by computer user account but not billed to individual users or their departments.

Faculty are encouraged to use a separate account for each sponsored grant or contract and to identify that project on the account request; normally, computing resources other than consumables should be treated as a UTD contribution in the grant/contract budget, but all resources will be billed to the sponsored agency upon request.

A detailed PRICING SCHEDULE is available upon request.

EXTERNAL ACCOUNTS:

- External accounts will be considered for government and not-for-profit organizations when a direct benefit to the teaching and research function of the University can be demonstrated, over and above any monetary compensation received; they cannot be provided to for-profit organizations; approval by the Vice President for Business Affairs may be required.

- Based upon joint agreements between UT system installations, users at other UT components are treated as internal users and issued either student instructional or faculty sponsored accounts.

- External users are billed at the statement rate plus a surcharge based upon the University's Overhead Rate.

- External users may also be subject to additional surcharges for the use of certain software packages (such as SAS or SPSS) in order for the University to fulfill its contractual obligations.

- If authorized by the Director of the Academic Computer Center, guest accounts may be opened for persons at other public or private institutions on a reciprocal basis if potential use of UTD resources is small and the performance, function, operation, administration or reputation of UTD's computing system may benefit these accounts are classified as administrative support.

OPERATIONAL DISCLAIMERS:

- In order to protect the integrity of the system for all users, the ACC reserves the right to close any account without notice; questions regarding the issuance or cancellation of student accounts should be successively addressed to the Director, Academic Computer Center, the Executive Director of Information Resources, the relevant School/Program computing coordinator (if one exists), graduate/undergraduate advisor, Program Head, School Dean, Graduate/Undergraduate Dean, and Vice President for Student Affairs.

- The ACC assumes no responsibility for the loss of user files, even if caused by ACC negligence, nor for preserving the confidentiality of user files; within the limits established by State/Federal law, the ACC reserves the right to examine any other user file in order to carry out the ACC's management responsibilities to insure the integrity of the system for all users.

- Notwithstanding the above, normal operational procedures should make possible the recovery of user disk files after system failure, account closure, user error, or staff error; tape files are NOT backed-up; users with particularly critical files or confidentiality concerns should seek ACC advice.