# Controlling Copyright Infringements of Intellectual Property: The Case of Computer Software - Part Two

This is the second of a two-part series. Part One (June 1994) reviewed the present status of intellectual property theft and global software piracy, discussed the dilemma of securing proprietary knowledge using legal means, and reviewed the activities of BSA and SPA, the two most prominent industry groups pursuing legal measures. Part Two discusses the legal and technological measures used to control piracy, elaborates on alternative solutions, presents the end-users' perspective, and makes recommendations for both IS software and user managers.

In a global economy that is increasingly information intensive, intellectual property is often the most valuable corporate asset and one that is particularly vulnerable to theft.
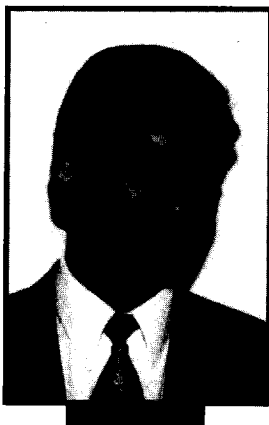
Yogesh Malhotra

Strategies for Controlling Piracy of Software

The strategies for controlling software piracy can be implemented by deploying technological solutions of 'protected' product design; by monitoring and regulation; and by using innovative pricing, distribution, and promotion.

These strategies aim to create incentives for buying legal software and penalties or disincentives for using unauthorized software. These strategies have been categorized into three main classifications: technological solutions, legal strategies, and pricing, promotion, and distribution strategies.

An overview of these strategies is provided in Table 1. The list is not exhaustive, but provides an excellent representation of various strategies that might be used to curb infringement of software copyrights.

Technological Solutions (Product & Packaging)

Technological solutions to prevent software piracy generally entail the use of an encryption process or other protective measures to protect the software. Hackers, due to profit motive or otherwise, enjoy breaking the copy-protection code of any newly released 'foolproof' software application. According to some software vendors, even the best-developed copy-protection code is susceptible to breaking within a period of a few weeks. The various technological solutions that can be incorporated in the product design or packaging are discussed below.

Technological copy-protection may be hardware-based, software-based or a combination of the two. Hardware-based copy protection techniques are most difficult and expensive to bypass. If a program is distributed contained in the ROM (Read Only Memory) of the computer, it offers strong protection against most thieves, but it also makes upgrading and maintenance of the program very difficult. Combinations involve identification by the software of some hardware component at the time of execution.

This type of protection can be rendered ineffective by disabling the verification routine which identifies the hardware. Software-based protection techniques, which rely on programmed code, are the most widely used and the easiest to defeat. These can be disabled by modification or deletion of the code providing protection.

Making Distribution Disks
Copy Resistant

This is one of the most popular types of protection for mass-merchandized software. It is done by varying the format of the data recorded on the disk. Recording on otherwise empty areas of the disk or by using areas of the disk that contain control information renders the disks incapable of being copied by standard software. The problem with this approach is that it does not permit creation of back-up copies even for legitimate users.

Access Locks

Access locks are programmed checks which verify that the software is being used on the right machine within the authorized license period and by the right customer. When the program is executed, a hidden routine checks for the expiry date, machine serial number etc. For example, a program may cease operating if the date or serial number of the computer does not match the legitimate 'keys' provided with the legitimate copy.

Recently, IBM announced that it will make available CD-ROMs containing as many as 100 different 'locked' programs at minimal cost to its customers. The customer can decide at leisure the software he or she wants to 'buy' and may execute the purchase by calling a toll-free number and receiving a decrypting code to 'unlock' the product from the CD-ROM.

Access locks can be used where software is leased or licensed for a limited time period, or is used for

execution on a specific machine. Generally, they are used with mainframes and for more expensive software. Access locks, just like any other software protection technique, can be disabled by a competent technician.

Encryption of On-line Data & the Federal Encryption Standard

With increasing distributed processing applications such as E-mail, large banks, insurance companies, and multinationals have started using encryption for preventing unauthorized downloading of their data from the networks. Numerous pieces of federal legislation have been passed to make it illegal for unauthorized individuals to tamper with files or computers in ways that may infringe on the legal rights of others.

Recently, the present administration announced that a voice encryption microcircuit called the Clipper Chip is to become the federal government's voice encryption standard for non-classified communication.

Hardcoded Numbers in Computer Memory

In one anti-piracy design technique, the software application runs on a computer only if it recognizes a specific serial number hardcoded in the memory of the computer it is loaded upon. The disadvantage of this technique is that the software can run only on one machine which it is designed to recognize. In case of a malfunction or obsolescence the software can not be used on another machine.

Software Resident 'Inside' a Read-only Memory Chip

In another anti-piracy tactic, which has been used by Texas Instruments, the soft-ware resides on a read-only memory chip. This prevents duplication of the code 'encased' inside the chip. This technique adds extra cost to the product and the software producer has to achieve a higher sales volume to generate the same revenue.

Copy-protection Security Devices

Increasingly, copy-protection devices are being made available to safeguard the software. Security devices available on the market tighten the security of the software. Some of these devices also keep count of the number of times a software is used.

Security keys, which are normally transparent to the users, prevent unauthorized use by an average end-user. They also provide means for programming the software to expire at a certain time or to block any further execution after a specific number of runs.

Use of Holographic Images on Software Packaging

Several U.S. software companies, in a bid to discourage piracy, started using holograms — which cannot be created without using million-dollar laser equipment — on their product packages. But, the pirates have been successful in creating high-quality copies of the holograms too.

Microsoft had felt secure that its release of MS-DOS (5.0) could not be counterfeited because it had used a holographic image on the product package, but raids conducted on a software counterfeiting ring in Taipei, Taiwan, proved otherwise. This ring had been responsible for producing

---

Table 1: Strategies for Controlling Software Piracy

(A) *Technological Solutions*
- Making Distribution Disks Copy-Resistant
- Using Access Locks
- Encryption of Online Data and the Federal Encryption Standard
- Hardcoded Numbers in Computer Memory
- Software Resident inside a ROM Chip
- Copy-protection Security Devices
- Use of Holographic Images on Packaging

(B) *Legal Strategies*
- Copyright Violations
- Proprietary Products
- Fair Use Doctrine and Educational Use of Software
- Shrink-wrap License and 'Broken Seal' Agreement
- Rental and Leasing of Software
- Interim Copying
- Piracy of Computer Typeface Fonts
- Multimedia and Emerging Copyright Issues

(C) *Pricing, Promotion & Distribution Strategies*
- Negotiated Agreements
- Reasonably Priced Back-up Copies
- Multiple Copy Discounts
- Licensing Agreements
- Commissions to Software Retailers
- Withholding of Source Code
- Institutional and Corporate Accounts
- Strong Focus on Customer Support & Maintenance
- Open Policy or No Copy Protection
- Free Market Solution (Let the Market Decide)
- Imposition of Levies

piraved copies of MS-DOS in English, French, German, Italian, and Swedish. Approximately $150 million worth of bogus Microsoft products, including holograms of impeccable quality, were being produced in China alone. Some estimates indicate that Microsoft annually looses about $1 billion due to the software piracy.

Most of the technological solutions of copyright protection are susceptible to failure by competent technicians. They can only provide temporary protection against software theft by average end-users. It is certain that technological solutions will merely supplement the economic, free-market, and legal methods of software protection.

Legal Strategies Affecting Software Copyrights

The legal system does play its role in controlling software piracy. But the legal solutions are not as effective as the free market solutions in controlling piracy of software.

Copyright Violations

In the fall of 1992, Congress amended the Copyright Act and made software piracy a felony. A minimum of 10 illegal copies of any copyrighted material is enough to convict a company. It has been pointed out that the new anti-piracy law does not distinguish between the three "degrees" of software piracy behavior: totally innocent copying, unfair use that might give rise to a lawsuit, and criminal piracy [6].

The new US Federal Sentencing Guidelines mandate in-place compliance programs. The wiser course for a firm accused of piracy is to submit to a voluntary audit which is far less expensive than the penalty imposed by the SPA which is usually the cost of the pirated software.

In a piracy case that involved MedPerfect (the software pirate) and Novell (the software supplier), the bankruptcy judge ruled that the bankruptcy law does not permit debtors to set aside debts incurred for "willful and malicious actions" [7]. The bankrupt MedPerfect was directed to pay Novell Inc. for sales of the pirated copies of the networking software NetWare.

Proprietary Products

Software companies face a dilemma in making their proprietary products public. For maximizing return on their investment they do not make the interface public. But, classifying an interface as proprietary to safeguard against the copying of the software results in a tactical marketing faux pas. A proprietary product may restrict the user's ability to use products from different companies and consequently restrict the product's potential market.

Many software firms that promoted widespread use of their commercial innovations have later declared their products proprietary and have demanded royalties from the users of those products. By disclosing the architecture of their personal computers in their earlier years, both IBM and Apple benefited because of the thousands of programs created by the third-party developers.

Copyrights and patents certainly provide the lead-time advantage to the innovator. Making an innovation proprietary compromises the interoperability of the software product, and by sacrificing compatibility diminishes its value to the user. Interoperability can be achieved by licensing or allowing the free use of program interfaces, protocols, languages, and other types of interfaces.

Paradoxically, some of the software applications that are most popular worldwide are the ones that had been most extensively pirated.

The 'Fair Use' Theory & Educational Use of Software

The concept of 'fair use' is one of the most important and least understood aspects of copyright law. The users (especially educators) need to have a clear understanding of what constitutes fair use of software programs, videotapes, digitized images and computerized text. The fair use provision states that copyrighted material can be used by educators (or others in similar functions) unless it infringes the copyright owner's ability to earn financial benefit.

The fair use provision is equally applicable to persons working for the non-profit sector and they may be held liable for duplicating software (or videotapes) without permission or for using stand-alone programs for multi-user applications on distributed networks.

Shrink-wrap License & 'Broken Seal' Agreement

Software companies are using the shrink-wrap agreement for legally binding the buyers of software products. Under such agreements, opening the seal of a software product by the customer binds him or her under the copyright law clauses listed on the package. Such clauses generally contain the number of machines on which the program can be used, number of copies that can be made, exclusion of rights to reverse engineer the program, etc.

Rental & Leasing of Software

The Software Rental Act of 1990 dealt a severe blow to software piracy committed by software lending libraries. Some of these libraries have been exploiting a loophole in the act and operating as nonprofit software lending libraries. SPA believes that these libraries are in fact a front for software piracy and has been investigating them closely.

Under the "grandfather clause" of the act, the original disks of the applications released prior to the signing of the Software Rental Act may be rented [8]. For software released after the passage of the act, exemptions include rental of original disks between two nonprofit educational institutions, and lending of original disks by a nonprofit library to another nonprofit institution.

Interim Copying

'Interim Copies' constitute copyright infringement. This decision was passed in the Sega Enterprises Ltd. v Accolade case decided in the US District Court of Northern California. Though the end products were dissimilar, the defendant was enjoined from marketing its video game because it had analyzed the plaintiff's software in the process of designing its own games.

Piracy of Computer Typeface Fonts

Font generating computer programs, such as PostScript or TrueType, are considered copyrightable and cannot be copied from masterfiles (from disks) for distribution. However, copyright allows one to scan an existing copyrighted font and sell it after modification. Typecase programs give the user a single printer privilege. This implies that more than one computers may use the software, but the font can be generated only on one printer. Additional licenses are required for using the typeface program on additional printers.

Multimedia & the Emerging Copyright Issues

With the increasing popularity of multimedia, new and more complex issues pertaining to copyrights for digital pictures (video clips) and digital

voice (audio clips) are surfacing. A major multimedia production may include hundreds of such clips, and using a computer, any picture or sound can be endlessly modified, printed, copied, replayed, and reused. Even most intellectual property attorneys are wary of the applicability of the copyright laws to multimedia. Based upon its research of experienced developers, the multimedia magazine NewMedia provides some advice for the users. A summary of guidelines often publicized for multimedia appears in Table 2.

Recently, Apple had been trying to address copyright issues regarding its Multimedia software QuickTime. Apple has allowed the distribution of unedited QuickTime movies in digital form only. Users could copy, edit and generally manipulate digital video QuickTime movies freely, but any other use has been restricted because the video footage belongs to its creator.

A possible solution could be the incorporation of the restrictions and replication rights for each QuickTime object in the software itself. Some companies allow copying and free distribution of video clips while others do not. The users should use discretion and make use of unrestricted material, or license the rights to the clips they need.

Pricing, Promotion & Distribution Strategies

Negotiated Agreements

Software publishers and developers can implement this strategy by using negotiated agreements with buyers for the purchase or lease of software. These agreements are subject to the doctrine of caveat emptor. Specifically, if the buyer is not sophisticated enough to negotiate the purchase or leasing of software, most software suppliers would not volunteer a discounted rate for things like multiple copies or back-up copies.

Reasonably Priced Back-up Copies

Most software media is destructible due to user glitches, natural disaster, theft, power surges, faulty circuitry, or computer viruses. Therefore, computer software copyright law explicitly allows the user to create a back-up copy which can be used if the original copy gets corrupted or destroyed. Users complain that several suppliers do not provide a back-up copy without an extra charge. Most users would be willing to pay a nominal fee for making back-up copies.

By providing this option, the software publishers can reduce the users' incentive to make pirated copies.

Multiple Copy Discounts

Another incentive that software publishers can provide to the users to dissuade them from making pirated copies is the provision of multiple-copy discounts i.e. discounts for quantity purchases. Certain software vendors are already providing discounts to volume buyers who meet their qualifications for site licensing or bulk purchasing.

Some computer resellers are forming consortia of smaller dealers and specialized resellers in order to gain larger discounts from distributors.

Licensing Agreements

Some software companies use licensing agreements to discourage piracy. In this case, the purchase contract prohibits the buyer from making copies. Some software publishers include a specific code in the purchase contract. This code is also 'written' on the software media and is replicated on to any copies that are created. Besides deterring the users from creating illegal copies, the licensing agreements also make the user aware of the illegitimacy of making unauthorized copies.

Varied licensing schemes used by software vendors confuse legitimate users who inadvertently copy software. Different vendors also have different policies for copying software for home and portable computers. To resolve these problems, vendors and user groups like SPA and Microcomputer Managers Association, are working together to standardize licensing schemes and to develop a standard interface for software metering in networked environments.

Commissions to Software Resellers

American software companies that include Adobe Systems Inc., Aldus Corp., and Autodesk Inc. are offering 20% to 30% commissions to software resellers to identify offenders of software copyrights. In most cases the company asks the offender to purchase the software and the reseller receives a commission on the transaction. Since it established its program in 1988, Autodesk has recovered more than $8 million by this process. More and more software companies are expected to follow the lead.

Withholding of Source Code

IBM has been practicing what they call OCO (Object Code only) policy of withholding the source code to protect software integrity and prevent theft of trade secrets. In the mid-eighties, IBM stopped shipping the source code with the software product. Even though IBM perceived the negative impact of their decision on the users, they did so to protect themselves from the uncertainty of the legal system. Users can no more customize the code to their own requirements.

Several third-party software developers claim that IBM's tactics are reducing competition by decreasing access to large parts of the IBM-compatible market.

Institutional and Corporate Accounts:

The software companies may lease their software to institutional clients

---

Table 2: Copyright Issues in Multimedia

a) Know which rights you are buying. Purchasing a physical reproduction of an image does not give the rights to reproduce, modify, or distribute it.

b) A person's image can be copyrighted. The identities and likenesses of fictional characters can also be protected under trademarks.

c) Proper clearances are needed from the copyright owners to reuse images originally created for another purpose.

d) Make sure to get permission for every object -- pictures, pieces of music, sound effects, etc. -- used in the multimedia production from the copyright owner(s).

e) Make sure to obtain all copyrights. For example, in the case of music, protection may include broadcast licenses for radio stations, sync licenses required for cuing music to movies, writers' and performers' copyrights on recorded music, and sheet music licenses administered by the copyright owners' publisher.

f) For your multimedia production, create as much of your own material as possible.

---

who may be allowed to make a specified number (or unlimited number) of 'copy-protected copies' for their users in return for a flat annual charge to the supplier. The institutional client determines the 'reasonable' price which it charges its users. The availability of legal software at reasonable prices dissuades the users from indulging in software piracy. Some computer dealers are following this practice in establishing corporate accounts for buyers who have average monthly purchases exceeding a specific dollar figure.

Several companies, including Aldus and Microsoft, use licensing agreements called 'license packs' under which the user can create multiple legal copies of the software. Microsoft, for instance, under its Extended License Agreement (XLA) allows a company to copy an application to all its computers if sixty percent of the company's machines are loaded with purchased copies.

Strong Focus on Customer Support & Maintenance

Statistics for the Commonwealth of Independent States (erstwhile Russia), a republic where widespread software piracy is evident, indicate that 21% of software is purchased with rubles, 11% is purchased with hard currency, and 68% is copied illegally. These figures can be attributed to high prices of software, poor maintenance support, and dearth of legitimate copies.

Availability of customer support coupled with low priced software may reduce piracy as it is evident from the case involving Magnit, a Russian joint venture responsible for distribution of Nantucket's Clipper software. Though illegal copies of the software are readily available, Magnit's sales have been increasing because of its focus on strong customer support.

Open Policy or No Copy Protection

In absence of an effective copy-protection system, some software publishers follow an 'open' policy to discourage piracy of their software (data or programs). The software is sold without any copy-protection! It is believed that serious users of software will reject continued use of pirated software if offered sufficient incentive to own legitimate copies. The software companies discourage piracy by providing frequent software upgrades to the registered owners and by providing a strong support infrastructure. Examples include provision of toll-free 'hotlines' to the users.

IBM had been planning to give away free copies of its initial release of OS/2 2.0 to users of MS-DOS and Microsoft Windows in order to captivate the Microsoft customers. The company had been planning to recover its software costs by providing the hardware upgrades required for using the software.

Recently, Apple had been moving away from its protectionist stance and had been planning on bringing the Macintosh operating system in public domain. It is emphasizing more and more on product differentiation by making its software smaller, less expensive and more specialized.

The Free Market Solution (Let the Market Decide)

According to the 'free market' doctrine, the success or failure of software packages should be determined by the free market mechanism. Customers want high-quality software at reasonable prices and they would determine the fate of any existing or new software. The free market competition would automatically squeeze out high-priced or low-quality software. The free market competition will undoubtedly make its impact in due course, though it is a relatively slow process.

Imposition of Levies

The software publishers can follow a process deployed by the television and motion picture producers to protect themselves from excessive profit losses due to video recorders. A 'levy' could be added to the price of software, the proceeds from which could be directed to the producers to offset some of the losses accruing from illegal duplication of software.

A different approach is used by the SPA's Copyright Protection Fund. This fund's membership includes well-known companies like Lotus, Microsoft and Apple. The fund fights software piracy on behalf of the entire PC software industry by taking action against businesses and individuals who pirate business applications, consumer software or educational software. Over the past three years, the SPA has collected more than $3 million in recoveries from settlements which have been used to fund future litigation and anti-piracy educational efforts.

Table 3: How User Managers Can Reduce Risks of Workplace Copyright Infringement

Negotiate with Software Suppliers for Unlimited Usage
Negotiate for License Packs
Define Policies on Software Use and Misuse
Establish Proper Controls to Ensure Legal Software
Conduct Regular Audits of Company's Hardware & Software
Prescribe Punishments for Copyright Offenses
Educate Employees About Software Copyrights
Develop and Establish a Software Code of Ethics
Use Asset Management for Tracking Software Piracy

Users' Impressions of Software Copyrights

Individual users believe that they are justified in copying software because they cannot afford the price of legitimate copies. Users also believe that they are justified in testing a program (preferably without incurring an expense, for example, by using a 'free' copy) before buying it. The software manufacturers consider both types of behavior as unethical. The issue of price was earlier addressed under Marketing Strategies.

Are there any solutions that software companies can devise which can provide the user a 'flavor' of the software before he invests in the purchase? Despite the software industry's attack on piracy, most users are unsympathetic to an industry that makes billions of dollars every year. Most users believe that software is overpriced and they cannot purchase individual copies for each machine. A perfect copy protection would not in-

duce them to buy software that they had earlier copied. Instead, they may switch to bargain replacements or inexpensive shareware programs which may drive down the commercial software prices.

Managers of user firms are frustrated and unhappy with the aggressive anti-piracy policies of SPA. They contest that the companies should not be held liable for the clandestine acts of software piracy committed by their employees. To check software piracy, some of them are negotiating with the software suppliers for unlimited usage of software applications in the workplace for a flat charge and lower 'license pack' and site-license prices.

Many have already initiated measures to curb software piracy in the workplace. These include education and awareness programs for the employees, defined policies on software use and misuse, regular software audits and prescribed punishments for copyright offenses.

Narrower Copyright Rulings

Contrary to earlier legislation, a recent decision handed by the Federal Court of Appeals in Computer Associates v Altai ruled that the basic structure of a program is not copyrightable — a program can take on the structure of the programs with which it must interface [9].

It further dictates that the parts of the program that belong in public domain, or constitute efficiency considerations, or are governed by factors external to the program, cannot be protected under the copyright law. This decision would encourage competition by reducing legal constraints faced by software developers.

In another highly publicized copyright-infringement claim filed by Apple against Microsoft Corp. and Hewlett-Packard, the courts ruled that only specific screen elements are copyrightable, not overall 'look and feel.' However, some court decisions, such as the recent ruling in the Lotus-Borland lawsuit that found Quattro Pro's macro key reader to have violated Lotus' intellectual property rights (because it allowed Quattro Pro to execute 1-2-3 macros), in fact deprive users of their intellectual property.

Recommendations for Software Publishers & Users

The legal enforcement of the new copyright laws and the prosecution of the offenders are the main stumbling blocks for software copyright laws in most countries. The legal process of controlling software piracy will follow its own course at its own pace. Emerging computer and software technologies will demand a further redefinition of the copyright and patent laws.

To keep pace with the changes, software companies will need to adopt effective pricing, promotion and distribution strategies to control software piracy. To reduce potential exposure to software copyright lawsuits, the IS user managers must imple- ment the proper software controls and conduct regular audits to ensure the legitimacy of the software being used on the company's computers.

User managers are also responsible for implementing all aspects of software policy, maintaining detailed records of software procurement, supervising compliance with software licenses, and developing a software code of ethics.

A company needs to have a published policy against copyright infringement, and software compliance should be a part of its overall trade secret protection policy. Software should be based on needs assessment, planning and budgeting, and established purchasing procedures, and should be suitably registered and secured. Most IS managers could save more than 5% on their PC software budgets by working out more favorable licensing agreements and controlling escalating software costs.

Asset management software can help IS managers track PC assets of all types and track the occurrence of software piracy [10]. A snapshot of the recommendations for the IS user managers is given in Table 3.

In face of increasing global infusion of information technology, progressive competition for customers, and the sluggish pace of the enforcement of copyright laws in various countries, software publishers will need to take an increasingly aggressive customer-oriented role to achieve competitive advantage.

They can accomplish this by pursuing innovative pricing, promotion, and distribution strategies. These strategies will offer incentives to the users for purchasing legitimate software and offer disincentives for making or using pirated copies. These innovative strategies should include negotiated agreements, reasonably priced back-ups and multiple copies, institutional selling,

licensing agreements, open policies, and, most importantly, a strong emphasis on customer support and service.

References

1. Weisband, Suzanne P. & Goodman, Seymour E. (1993, October). Subduing Software Pirates. Technology Review, pp. 30(4).
2. Depke, Deidre A., & Yang, Dori Jones. (1989, December 25). Casting a Worldwide Dragnet for Software Pirates. Business Week, p. 54H.
3. Husch, Tony, & Foust, Linda. (1991, September). Protecting Your Ideas. Nation's Business, p. 92.
4. McCauley, Peter. (1991, September 16). The pluses of patents. Computerworld, p. 23.
5. Schwartz, Evan I. (Ed.). (1990, November 19). And Congress Gives Software Makers A Break. Business Week, p. 138C.
6. Kapoor, Mitchell. (1993, February 15). Innocent Felons. Forbes, p. 208.
7. Ubois, Jeff. (1992, Sept. 28). Piracy Fight Finds Many Battlegrounds - Congress, Courts Are Main Arenas Now. MacWeek, p. 46.
8. Picarille, Lisa. (1992, Jan. 13). Firms Exploit Loophole In Rental Act. Infoworld, p. 2.
9. Brandt, Richard, et al. (1992, July 20). Bit by Bit, Software Protection is Eroding. Business Week, p. 86(3).
10. Francis, Bob. (1993, June 1). Automate Your Asset Management. Datamation, pp. 47-50.

Yogesh Malhotra, MBA, CDP

has consulted in management information systems for Fortune 100 and multinational corporations that include BankAmerica, the TATAs, and the Unisys Corporation. His articles on MIS issues and multimedia have been accepted and published in American and British journals. Presently, he is pursuing doctoral education in MIS at the Katz Graduate School of Business, University of Pittsburgh. E-Mail: MALHOTRA@VMS. CIS.PITT.EDU