The Need for Ethics Education in Computer Curriculum

John A. N. Lee

TR 91-25

The Need for Ethics Education in Computer Curriculum

by

John A. N. Lee[1]

Abstract

The availability of the computer to a broad section of the community has brought under its influence a number of individuals who may not have been so well disciplined in appropriate ethical behavior. Lacking precedents and truly parallel paradigms as in driver and sex education, this paper recommends that earnest consideration must be given to introducing ethical concepts and case studies into secondary school classes as well as in professional school curriculum related to computing. Surveys have shown that the person most likely to have misused a computer/communication system is the employee of the company under attack. It is the responsibility of the computer community to reach as many of these employees during their formative years to divert them from inappropriate practices. The objective of this paper is to consider the state of affairs in computing which lead to deep concerns about ethical behavior and to present proposals for the inclusion of ethical concepts in early computer related courses.

CR Categories and Subject Descriptors: K.5.0 [**Computing Milieux**]: LEGAL ASPECTS OF COMPUTING - *general;* K.3.2 [**Computing Milieux**]: COMPUTERS AND EDUCATION - computer and information science education - *computer science education*
General Terms: Experimentation, Human Factors, Legal Aspects, Management, Reliability, Security
Additional Keywords and Phrases: Hacking, Viruses, Intrusion, Ethics, Ethical Behavior, Curriculum

---

[1] Author's Address: Department of Computer Science, Virginia Tech, Blacksburg VA 24061.

What we dream up must be lived down, I think.
- *James Merrill*

Introduction

With the introduction of an affordable personal computer in 1980[2], the teaching of computer related topics in the public school system has taken its place alongside sex education and driver education classes. At the same time a new sport of computer abusing has emerged through the concomitant access to public communications systems. While we have no more evidence than anecdotes that these two phenomena are interrelated, the schoolroom may be one of the few places where the ethics of computer usage can be impressed on students. Like sex and driver education, computer education will teach facts and skills, and from there, in the classroom community, develop interpersonal relationships leading to the need for moral and ethical decision making. However, unlike sex and driver education no claim can be made that computer education can also be effectively accomplished in the home rather than the schoolroom. Dissimilar from either of those other activities, few parents have adolescent experiences of their own to build on and to be able relate to their offspring in such personal terms as "*you can't fool me, remember that I was 14 once*"! Even in those family situations where one or more parents are professionals in the field of information processing, they often do not have the same exploratory nature as an adolescent to find out "how it works".

A teenager is surrounded with derogatory examples of the fact that nobody seems to obey the rules. They have been brought up in a world where, from the first day they were brought home from the hospital, the culture permits one to exceed the legal speed limit - by just a little, or when the radar detector reports no radar surveillance. The fact that there is such a good business in making and selling radar detectors is itself a measure of the acceptability of deviations from the standard when "Big Brother" is not watching! Before young people go to school for the first time, they have at least witnessed the profusion of slightly illicit relationships in TV soap operas, and during their teenage years have glimpsed the shenanigans of late night shows. Even in those cases where parents have restricted and controlled TV watching, children are exposed to undesirable elements through osmosis from other, not so protected, peers. The prevailing societal attitude is to get away with what you can. Exceeding the speed limit within the acceptable tolerance of radar detectors (and the credulity of the traffic court judge) is permissible. Slipping into an R rated movie by claiming to be two years older than you really are is acceptable, knowing that your parents will react in a non-punitive manner when they find out. Boys found smoking behind the barn is a standard scene on "Little House on the Prairie" style films. But in both sex and driver activities a danger exists that goes beyond just getting caught. Real terrors need to be avoided, risks must not to be taken lightly, and life changing injuries must be circumvented. By the time the student has reached the age of puberty and eligibility for a driving license, he/she knows that the forthright message is to "*do as I say, not as I do*". And anyhow, no-one plans to get caught; rather the planning, if any, is how not to get caught.

---

[2] Before 1960 most computers permitted immediate user interaction; the need for the "efficient" use of high cost machines introduced operating systems and banished the user from the computer room until about 1980 when the computer room became the family room.

Computing is a risk-free activity. There is a lack of fear of retribution from the computer, or from the communications system to which it is connected. Perhaps we have gone too far in demonstrating the robustness of computer systems by saying "*go ahead, you can't hurt it!*" At the same time we learn that a computer doesn't hurt us either[3]. Only in tabloids can computers electrocute the chess players who are surpassing them. You cannot even destroy your own computer with errors and mistakes, and bugs exist in almost all programs without affecting the overall health of the system. One can catch a virus from unhealthy activities, but the impact is on the computer, not on its owner or user. While our normal ethical conduct is controlled by the impact that we observe in others, the remoteness of computing and the lack of perception of effects provides none of the normal feedback related to behavior control. Robinett [1991] suggested an analogy, or parallelism, by likening the psychology of remote computing to "*the same kind of distancing that occurs in the development of weapons that allow us to kill without having any personal contact with the person who dies.*"

This paper reflects on the environment that we have created for our young people and suggests that our prime responsibility is to include in our teaching about computers and computing some of the same moral and ethical teaching with which we accompany sex and driver education. In the same manner we must balance the teaching of facts, skill and capabilities, with an understanding that we are opening a Pandora's box that may be difficult to not open the whole way! Does the teaching about inappropriate acts lead to the activation of those acts? The objective of this paper is to answer these concerns and questions, and to reflect on potential topics for studies of ethical behavior which may be included in early computer related courses.

The Risks

With the advent of the personal computer, no longer was it the privileged or canny few who had access to teletypes and who could access main frame computers. Even the smallest computer, costing as little as $100, could be coupled to the family TV and to a modem to provide an electronic tripping medium for the new breed of hackers. And this new breed did not build on the knowledge of the advances made by their predecessors. They had the equipment, they had the urge and, most times unbeknownst to their parents, they acquired the knowledge to travel the world without leaving the privacy of their bedrooms. No-one provided a code of ethics for their wanderings because their teachers were not sufficiently knowledgeable of the potential of this combination of computer and modem, and their parents had no adolescent experiences of their own on which to build an expectation of the outreach of their offspring. A computer education package is needed that has similar moral and ethical scenarios as would be found in high school courses in driver education or sex education.

As the owner of a personal computer extends his awareness and knowledge of the system, several paths emerge that can lead to further insights and to further exploration: to install or develop new software packages, or to explore other people's packages. Given the limited resources of a teenager, the former is not easy to acquire

---

[3] There are obviously some cases where a computer is in control of a situation that impinges on human health and welfare where this is not true. The Therac 25 case, for example [Joyce, 1986]. However, very few students have authorized access to such environments.

unless currency can be exchanged for other possessions. Bulletin Boards were an early development for communication between PC users, but by their very nature they required the possession of an environment that permitted a wider latitude of exploration than just a bulletin board. Some of these boards also became (and still are) the repositories of software packages, many of them donated to the public domain by their developers. In other cases, proprietary or copyrighted packages were available for some small cost - either in exchange for some other unique piece of software or, in one documented case, a mere identification such as a credit card number. Though the board owner promised not to charge the card for any software, the card number did get used in other nefarious ways without the owner's prior knowledge. In many cases, of course, the card number belonged to the parent of the provider.

These kinds of activities, particularly when noticed by the news media, have been labelled as "hacking":

> **hack** (hak), *n*. 1. a horse for hire. 2. an old, worn out horse. 3. a literary drudge. 4. a coach for hire. 5. a taxi cab. *adj.* 1. employed as a hack. 2. trite. *v.t.* to chop or cut roughly. *v.i.* 1. to make rough cuts. 2. to give harsh dry coughs. *n.* 1. a tool for hacking. 2. a gash or notch. 3. a harsh,dry cough. - **hack'er**. *n.* - **hack'ing**, *adj.* [4]

The concept of hacking as a methodology to achieve some particular goal has the allusion of working at something by experimentation or empirical means, learning about the process under review, or development by ad hoc mechanisms. This may have had an origin from the use of the term "*v.t.* to chop or cut roughly. *v.i.* to make rough cuts" as in the process of empirical development where numerous different routes are explored in a search for the most effective approach to a solution, but without necessarily having planned an ordered search or necessarily a methodology for evaluation. To chance upon a solution through "hacking through a problem" is often as educational as structured learning, and thus approaching a problem in a field which is devoid of structure and methodology by "hacking" is not considered to be unreasonable. In hacking a computer, the enhancement of the system is an end in itself - applications of that system don't count. In the same manner, hacking has no life cycle and no specific end goal; an improvement is in itself an achievement, but not necessarily a reason for further activity. While hacking was generally counter-society it was not necessarily anti-society. The result of hacking is a "hack" and the beauty of a hack can only be realized if others can share in its beauty; the private hack is nonexistent.

Hacking is not restricted to computing and by no means can we suggest that hacking starting with computing. Computing has merely provided a readily available resource for a wide range of "hacks". Levy [1984] and Dorsey [1990] documented many non-computer hacks actuated by "Techies" that not only demonstrated their prowess in using their resources but were so clever as to create a strong sense of forgiveness in those on which they were perpetrated. On the basis of the cleverness of the hack, the ingenuity shown, and the minimization of a residual cost of clean-up, most hackers (even though unknown) were lauded for their exploits. Within British university communities the "hack" has been the anticipated highlight of "Rag weeks" since their imposition has been for a good cause - the raising of funds for charities! Thus, though sometimes a minor inconvenience, the "hack" has a

---

[4] Websters New World Dictionary, 1967.

noble, innocuous, unoffending and inoffensive historical base! Why then has the computer "hack" strayed off this benign line?

Whether it be societal development or anthropological progression, the teenage period has become the period in which young people begin to learn more about the world around them as they prepare to leave the family fold. This period marks the time when they must find their niche in life and by timorous steps begin to learn how their personality and capabilities will provide them with vehicles by which to create a livelihood. Even without much direction from adults, teenagers become explorers, testing the boundaries of their current world and discovering new domains that are now open to them by virtue of the simple chronological progression of their age. Changes in metabolism cause common place features to be seen in a different light, and recognition of impending maturity by peers and seniors allows them insights that were not recognized earlier. An examination of this era for the purposes of systemization must lead on to suggest the introduction of an underlying Teenage Creed:

> *To discover and learn about the world and each other - by exploring, testing and trying*

From an adult point of view this practice is not without risks. Not all domains have neat, well defined borders; some domains have fences over which one can look but not participate. There are open doors that are not to be entered, while there are others that have a welcome sign hidden behind them. These adolescent activities are as applicable to automobiles and sex as they are to computers and communications. Ralph Waldo Emerson is credited with having suggested[5]:

> *Minds stretched to a new idea never go back to their original state*

If Emerson did make that suggestion then I am sure that he had the positive concept of mind stretching, but the concept is equally applicable to negative activity. Just as the country worried in 1918 about how *"are we going keep them down on the farm?"* - referring to GI's whose minds had been stretched by "Paree" - so, minds that have been stretched inappropriately must be of concern. Unlike an open door to a restaurant, the home telephone does not have a list of charges hanging alongside it so that the teenager can distinguish between the MacDonald's of communications delight and the Ritz. To have to ask about something is to admit ignorance and immaturity, and so only by surreptitious exploration can the stigma of ignorance be avoided. In other cases the lack of prior approval implies permission to repeat the action with minor aberrations. How delightful it is to see a youngster talking to grandmother by long distance telephone, and the encouragement to prolong the conversation when parents suggest that *"you didn't have much to say to Grandma!"* Then why is a conversation with a friend so much different? Having been given permission to do something once is to be taken as global permission forever! The problem of needing to appear to fit in, to be an upstanding member of this community, or to locate some section of the community in which one can find acceptance and recognition is fundamental to the teenage society. Youth groups often concentrate on small group activities and pre-planned rewards so that everyone has the opportunity to excel in some way. The activities of game playing (football, soccer, hockey, swimming, baseball, etc.), school societies (French club, FFA, homemakers, etc.), national organizations (Boy/Girl Scouts), church

---

5 Perhaps erroneously attributed since so many quotations are misattributed to Emerson.

organizations (bible class, Sunday school) and even pick-up groups provide a restricted community in which each person can act out the actions of a lifetime with definite rules and rewards. Goals and achievement levels within such groups provide visual evidence of the rites of passage towards adulthood. Service as an officer in an organization provides a demonstration of power and leadership. Attainment of collectively approved goals releases the participants from peer pressures of progression and permits the passage to the next level of discovery and exploration. Adolescent needs can be categorized as:

the rights of passage,
the demonstration of power or ability,
and the release from peer pressures

The rights of passage include learning to drive, and that first sexual encounter. To miss out on these rights of passage is to be ostracized by the peer community; to be ostracized demonstrates the need to find a more compatible society or to establish a lone identity.

As a loner, the hacker divorces himself from the community but with the outstanding desire to observe the activities within the society. While he has few of the social graces that make him acceptable to the community, his most ardent aspiration is to know all there is to know about that community. To know requires access to information on a timely basis and that often implies the access to otherwise privately held information. Whereas the mere size of physical hacks required the membership in a brotherhood to support the myriad of physical and logistic subtasks of prosecution, a computer hack is supported by a very able assistant - the computer itself. Computer hackers *"are not part of the community in any real sense. The image of the hacker as the lone cowboy, who rides into town, takes what he wants or needs, and rides out again, makes this lack of community sense clear."*[6] The actions of *"riding into town and out again"* can be achieved electronically without leaving the seat in front of the computer, thereby distancing the activator from his prey.

Positive Alternatives

If in 2000 years from now one were to examine the fossilized artifacts from today's school, the anthropologist would find that the majority of artifacts were models of reality, or playthings. Only one device is so real, and so powerful. Albeit that such devices are commonly limited in resources, they do provide a view of a larger reality and the opportunity for small excursions into that wider world. Perhaps only Nintendo® style games have had as much impact, but the tools to modify and create games are not generally available. But closeness to reality can also bring frustrations of ownership. Toy machines are soon outgrown, and in their place grows a need to learn about and use real machines, real systems and real communications. Students only get to nibble at a corner of the real world - they want to reach out for artificial intelligence, neural nets, communications or whatever is the latest fad or development. Apple Computer Corporation, for example, created a demand for Hypercard 2.0 by delivering systems late in 1990 that contained a "read only" version. My suspicion is that many users, having once been titillated by that "freebie", obtained updated versions illegally.

---

[6] Robinett 1991

® A Trademark of ....

An obligation of any course of study of computing must be to identify positive alternatives that will in turn provide acceptable activities to relieve the frustrations of limited educational domain. These alternatives must provide outlets for desires, an environment for controlled experimentation, a system that will provide a sense of achievement, and some form of access to the *real* thing. The sense of frustration is engendered by the knowledge that there exists a new domain to explore which has capabilities and opportunities that are so close and yet so far away. When we examine facilities and resources available in the community, we can note that in many cases large scale systems are not fully used outside of the normal working day. This suggests that with a little ingenuity access to modern, up-to-date equipment could be as close as next door! The fear in the minds of potential providers has got to be "*would it be possible for me to provide access without compromising my security?*" or "*if I once provide access, am I committed to a long term relationship at ever growing cost*?" Take, for example, computer vendor showrooms. In most cases such establishments contain the latest equipment on show to potential customers, but outside business hours the equipment is unused, or only lightly used. Such systems are probably not as liable to security restrictions since they are not used in ongoing commercial activities, do not store sensitive data and are not connected to data lines. From the student's point of view the changing nature of a computer showroom is an advantage - there are almost always new roads to explore! From the point of view of reportable achievement and prowess with using the latest technology, such installations are ideal as alternative outlets for inquiring minds. This positive alternative was recommended as part of the ACM Hacking Report in 1986 [Lee, Steier, and Segal 1986] but, as far as we know, has never been implemented even though representations were made to some vendors.

Schools and universities have become particularly skeptical about permitting access to the machines that support their record systems, and yet these very systems are of the type most likely to be used by graduates of these institutions. Instead students are relegated to "toy" systems. In some ways denying access to such local systems is tantamount to challenging hackers to break into them! But a risk analysis alone will reveal whether it is preferable to try keep everyone out and risk unauthorized access by the brilliant few, or to provide common access and thus increase the population with the potential for electronic exploration. If only the security of such systems could be improved at a reasonable cost and with little impact on the usability of the system for the general working population, alternative solutions to the hacking problem could be created.

Our reason for concern about denying access, or controlling access to systems, or conversely providing controlled access to a system, is based on the assumption that whatsoever we permit or encourage within a learning environment will be tried and tested outside of that environment. Why else do we learn, except to apply those skills in other environments? Schoolwork becomes life's work. That which we permit or encourage now, will proliferate into the future. Once again we should compare computer education with driver and sex education. Jim Horning commented "*good judgment comes from experience; experience comes from bad judgment*". How does one provide an environment in which experiences can be fostered while judgments are applied, and at the same time protect the student from the dangers of application? Does merely talking about a concept in the abstract replace the desire to act concretely? Can understanding be complete without practice?

The Psychology of Remote Control

The Smithsonian Institution, National Museum of American History, opened a new gallery in 1990 entitled "The Information Age". Replacing a 1960's gallery that featured the development of the computer and which included elements of such early machines as ENIAC and Whirlwind, this new gallery commences with two tracks that document early communications and early computation. Shortly after World War II these two streams intermingle, the one becoming interdependent on the other. On the side of telephonic communications, the computer saved a whole generation of young ladies from being employed as telephone operators and put the responsibility for the interconnection of telephones in the hands of the user (literally) who had to remember and "dial" the communicants access number. The complexity of telephone networks and the need to find alternative routings during times of overload or disruption also necessitated the introduction of the computer into the telephone system. As computers became more powerful, and for a period more expensive, telephone communications solved the problem of travel and simultaneous access for many potential users.

With this joined access came what we might term The Heisenberg effect of network communication. Immediately computers appeared in personal offices, laboratories and even in homes. No-one was standing in line (in the dining room) to use the terminal and no-one was looking over your shoulder to see what you were doing. As means to communicate between users was implemented, electronic mail over wide area networks emerged. This Heisenberg effect can be identified as the effect of the segregation of command, control and effect. In this situation one finds classic manifestations of the proverbs "*what you don't see can't hurt you*" or "*out of sight, out of mind*". The psychological impact of network communication [Shapiro and Anderson 1985] turned usually passive users into network demons, free of the controls and attitudes of eye-to-eye communication. Mice became lions overnight! Similarly, mice found the anonymity of hiding behind a computer and a communications line. Separation of the user from the provider of service, and from the possible recipient of communications, seems to have brought out underlying emotions that had lain dormant until this open system was presented. We see the effects of the openness of computer/communications systems on all levels of professionalism; just the effects and degree of inappropriate action vary, perhaps limited by more a respect for the machine than the person! Our experience reveals a significant difference in personal attitudes between people on the same phone line when using a computer to communicate or when using voice. E-mail communications are packaged; no response emanates from the recipient until the whole communication package has been transmitted. With voice communication (except to a telephone answering system) the recipient can interrupt at various levels of ferocity.

Within many university communities the computer network and communications systems have become indispensable to the essential activities of the institution from administration through research to teaching and learning. As we move into multi-media applications of computers and communications, the whole university experience in hard and soft sciences, in engineering, business and the humanities will be affected and it will be no more appropriate to restrict computer/communications usage then, any more than we can impose restriction today to prevent inappropriate usage. Universities would find it difficult to continue their work in education and research using restrictive systems. Such systems must

reflect the concept of a university as a place for the free and open exchange of ideas, and the open and free experimentation with model organizations. Security can be implemented by various means; shielded hardware and regulatory software are among the most common safeguards. Two challenges [Irwin 1990] appear to have proved that secure systems are feasible at reasonable cost. However, increasing the level of security can mean a corresponding diminution of services. A computing center director will have to determine an equilibrium between his expenditures on hardware/software security and the encouragement of more responsible uses of the equipment under his control. The fear of intrusion must be balanced by the support of education while recalling that the most likely direction of attack will be from inside!

Compulsive Computing

The psychological impact of computing, programming, networking, and communicating can be recognized in numerous manifestations of human reaction, especially as noted in the previous section. Another impact, which was recognized very early in the history of our field, is impulsive computing. The addiction to computer-related activities may be the result of the siren call of irresistible power and the sense of accomplishment that is the consequence of the use of that power. The addiction to any icon is questionable, though suitably channeled addiction need not be unnecessarily negative. However experience with other addictions suggests that addicts reach a stage where extension of the addiction to a new high or to another level is irresistible. Thus the fear of creating addicts of computing among our students must be muted by the availability of a stepped series of exercises that provide the students with accomplishments that continually satisfy the needs of those students. The field of computing and communications is now broad enough to lead to a lifetime of learning; part of our educational process must be to point to the next appropriate challenge.

Why Viruses?

Viruses, like the term hackers, have become the byword of the recent years. Viruses and hackers seem to go together. Contrasted with logic bombs and trap doors, viruses have the basic characteristic that they replicate under certain circumstances and thus are said to "infect" other software items. Viruses themselves may have two potential purposes - to replicate themselves and to perpetrate some mischief as a bomb or a worm. On the other hand, a virus may do nothing more than replicate itself. The minuteness of simple viruses means that they can be embedded in other systems quite easily and any differences in file size may be attributed to version differences. A common technique is to embed a virus within a commonly used system and to modify the initial load module to link to the virus before starting up the application. By attaching themselves to word processors or spreadsheets the likelihood of invasion by a virus is greatly increased. Viruses can be introduced into a system by a variety of doors. A system connected to a network is liable for entry through e-mail, through the linkage to other infected systems, and through bulletin boards to download software. Viruses can also be carried in on diskettes that have be used in infected systems. Attractive software, commonly to be obtained illicitly to circumvent copyrights or protective locks serve as "Trojan horses" and carry with them the virus. One particularly obnoxious form of virus is the "worm" that has the characteristics of eating its way (by destroying data and programs) through the storage system of a computer. Antidotes to viruses have been constructed for many of the well known versions and a new industry has been created to build virus detectives, immunization procedures and antidotes. Like safe sex, there are virtues

associated with obtaining software and data through well known, legitimate sources! Abstinence is also a virtue! Practice safe hex!

The attraction of developing a virus as a personal project derives from the fact that viruses are among the most challenging software to develop. Not only are there the challenge of producing a system that reproduces itself, is miniature and invisible, yet powerful and resistant to detection and modification. To be successful most viruses must access the supervisory mode of the victimized system and beguile the operating system into believing that they have privileges that permit their entry to the complete catalog of programs, applications and utilities within the organization. To masquerade as, and to operate at the supervisory level is an achievement greatly to be desired! Thus viruses present themselves as challenges whose defeat is a mark of achievement that can rarely be attained through "plain" programming activities.

Why Protect Software?

In the year 2000 computers will be given away to sell software[7]

In the beginning, computers were delivered naked. It was the user's responsibility to write the programs that were needed for their application. As the first programming tools were developed by the vendors, they were provided freely; user groups were formed which, with the assistance of the vendor, exchanged programs through a "library". User groups also formed cooperatives to develop special software and challenged their vendors to implement new systems to their requirements. As the cost of hardware decreased in accordance with Grosch's law, there was a commensurate growth in both the size and complexity of basic software, as well as its cost. As the cost of the basic software needed to support a computer system grew to be of the same magnitude as the cost of the hardware, vendors realized that they could no longer afford to hide the cost of software within the cost of the hardware, so software was "unbundled" and the birth of a distinct software industry occurred. Computer programs, applications and systems took on property rights and provided an advantage to their owners that could be exploited commercially. Software (and data) developers and owners began to recognize the inventory "value" of their possessions, especially when those holdings demonstrated new departures in extending the usability of the computer. Software companies, like the record industry, could only prosper if they could control and benefit from the physical manifestations of their products. Intellectual property rights in the form of patents, copyrights and trademarks - the established mechanisms for the protection of hardware - were applied to software. The expectation was that the penalties for misuse would provide the security necessary to establish a financially stable commercial operation based on protected commodities.

Free software was not available to "the common man" since there had been no need for him to acquire software for a non-personal machine. Thus one cannot put the blame on the violation of property rights by the copying of software on the established norm. An established norm however existed in parallel products such as audio- and video-recordings for which there existed simple means of reproduction. Like the stereo-player, most personal computers were provided with two read/write disk drives, and the copying of diskettes for "backup" was not only encouraged but, in many cases, mandated by not totally reliable systems. The tools and practices of copyright violation were built-in to the majority of systems. At the same time the

---

[7] Howard Aiken, quoted by Henry Tropp.

cost of software exceeded the pocket change of not only teenagers but also professionals! Truly useful systems, such as Lotus 1,2,3®, involved major expenditures that were not to be taken lightly; computer games were no less expensive than packages for specialized systems. And even though computer store and mail order enterprises have become widespread, the ready availability of a piece of software in someone else's system *when you want it* promotes copying. Estimates in the trade press suggest that so-called software piracy in the USA produces two copies of every piece of packaged software for every legitimate sale. Estimates in other countries where access to authorized sources is far more difficult, place this proportion of improper to valid copies as high as 20:1. But like exceeding the speed limit and cheating on income taxation, copyright violation is practiced at all levels of our society in order to meet the immediate needs of the moment. Faculty copy software for students because they need to have an exposure to such systems as part of their education and the institution has been unwilling, or unable, to acquire site licenses for every piece of software available! Software has not yet been made available in libraries for loan since, once acquired, it is difficult to return to the library stacks. New software, or updated versions of well used software, appear with such regularity that acquiring individual site licenses for software to be used in schools and colleges could be a full-time task for a software librarian. Some companies have provided "educational versions" of their software that can meet the needs of most classroom experiences, but this availability only extends to the need to acquire the "real" system through nefarious means.

The protection of private data raises different questions to those of protecting software packages. Whereas software is generally intended for wide distribution, and there are some packages of data such as demographic information that are accessible, private data as saved by commercial organizations is intended to have a restricted domain while maintaining a high replacement value. That is, commercially stored data essential to the effective operation of a company may not have any intrinsic value, but would be extremely expensive to replace. Private, personal information relating to employees and customers requires protection from outside intrusion in much the same manner as the trade secrets of the company are protected. Similar data stored by governmental agencies for the execution of their assigned tasks exists in an enigmatic environment where a democratic government is subjected to the freedom of information requirements so as to not govern by means of information not available to the "loyal opposition". At the same time the government expected to protect detailed information pertaining to individual citizens. The acts that permit the freedom of information do not, however, imply free and unrestricted access to information but instead that appropriate information should be available properly. Citizenship in a democratic society implies the protection of one's personal autonomy, invulnerable communications, and safeguarded storage of personal data. Contravention of these rights by others is unacceptable to inhabitants of a democratic society. Like the locksmith profession, the information technology community has provided society with the double edged tools of reasonable and unreasonable data access. The responsibility of the information technology community must be to provide the means by which these tools are used correctly. In the extreme this raises the question of Orwellian "thought control" that has plagued computer ethicists for a considerable period. Consider the question that can be posed to compiler implementers: *"should the compiler permit the use of translated programs which are likely to give erroneous results?"* or to data base managers: *"should data base processors permit the attempted correlation of data sets which are*

® Registered Trademark of Lotus Development Corporation, Cambridge MA.

known to be independent?" In general, we need to find a means to answer the question *"should we permit uncontrolled experimentation with computer and communications systems, so long as no harm is done?"*[8] Answers to all these questions may depend on our knowledge and acceptance of a code of ethics.

Codes of Ethics

Following the exposure of the internet virus introduced by Robert Morris in Fall 1988, there was a profusion of publication of "ethical statements" by such organizations as EDUCOM and the National Science Foundation [ACM 1989]. Codes already existed in the repertoire of the professional information science societies - ACM, IEEE and DPMA [Johnson and Snapper 1985]. Few members realize that they agreed to uphold and conform to those codes when they placed their signatures on their original membership application forms! An examination of these codes will reveal that they are basic derivatives of the most fundamental guideline:

A breach of common sense is a breach of a <society> rule

The ACM code includes a set of disciplinary actions that might be taken against a member who is found to be in violation of the code. However in the many years since they were promulgated, ACM has neither questioned the actions of any member and thus never applied these disciplinary actions. Whether this attests to the high ethical standards of ACM members or the inability (or reluctance) of the Association to prosecute a violation is not clear. Such codes were written in an era when (1) the majority of computer software developers were members of one of the societies and (2) the problem of computer/communications misuse was still unrecognized. Before 1960 while computers were personally interactive, the access to computers and communications systems was severely restricted, and while hackers existed, their desires were being satisfied by the creation of systems that we would find mundane today but which attacked the leading edge of development at that time. Even after time-sharing and interactive computing were introduced by such undertakings as CTSS and Project MAC, and computers and communications became inexorably interconnected, the originators could not accurately predict the future of computer misuse[9].

After a study of the world of hacking in 1984[10], Steven Levy documented the Hacker's Ethic:

> *Access to Computers - and anything which might teach you something about the way the world works - should be unlimited and total*
>
> *Always yield to the Hands-On Imperative!*
>
> *All information should be free*
>
> *Mistrust Authority - Promote Decentralization*

---

[8] The 1990 British Computer Crime Act outlawed even *attempts* to access closed systems.

[9] David and Fano 1967.

[10] Levy 1984.

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position

You can create art and beauty on a computer

Computers can change your life for the better

The open systems imperative within the MIT (TX-0) environment of 1960 and the Bell Labs (UNIX and C) environment of 1970 encouraged the review of the activities of peers by the browsing of unprotected files. This imperative opened the possibility that partially developed processes could be improved, corrected and expanded freely. Some systems were debugged overnight to the delight of the originators. This suggests an additional Hacker Ethic:

You can always make things better

In partial response to one of the questions disclosed in the previous section regarding the borderline between ethical and unethical behavior, one must recognize an additional ethic:

What you don't know can't hurt - If no harm is done, then there is no ethical violation

Ethics in the classroom often exists in terms of a set of school rules that are intended to supplement the basic law of the community in which the school resides, and which now apply to the specific school community. Such rules, like those of the professional societies, were not designed, and probably cannot be easily modified, to take into account the ever changing technological community. School rules relating to the use of motor vehicles simply were not required when students did not arrive in cars. School rules do not need to overrule the basic rules of a family unless those rules permit actions that contravene the basic mission of the school. Very few schools had rules limiting interpersonal (bordering on sexual) guidelines before the "sexual revolution" of the 1960's. On the contrary, schools had unwritten rules that expelled pregnant teenagers (their presence being disruptive to the school discipline). Bedroom activities, on the other hand, were still under the control of parents. But bedrooms are commonly the place where parents and their children have installed their computers and communications interfaces! The majority of secondary school graduates do not enter professional organizations that espouse codes of ethical conduct, and thus school honor codes must be the basis of the code of ethics of the majority of adults. Similarly, the majority of computer users will never be eligible to join an information technology professional society and any ethical decisions they make will be based on their prior or parallel experiences that relate to ethical behavior. Just as was used in the fight against drug usage, so we must expect that schools provide sufficient information and background in ethical guidelines at least to

know when to say no

My guess is that at least 90% of all programmers, working in a large number of organizations whose activities have a profound impact on our daily lives, are not computer science college graduates. Programming is not a profession that is subject to standardized testing and certification. A very large number of those working as programmers got their education either from high school classes (in BASIC), from professional institutes, from on-the-job training, or simply by osmosis. Their

training is often limited to the exact technical skills needed to qualify for the task in front of them. Apart from missing out on a plethora of associated educational experiences, students whose primary objective is job training rather than education are not exposed to the ethical expectations of the trades into which they are entering. Apart from some specialized organizations, or companies within the industry of information processing, few employers have the experience to vet the qualifications of their potential programmer employees. Many employers may be unwilling or unready to verify the training and capabilities of programmers[11]. Employers have a right to expect more than just technical training from graduates of professional schools, but do not get it. Thus secondary schools are the only common place where the basis for ethical guidance can be introduced.

Computer Education

Computer education today must minimally include problem solving, programming, and ethics. It is incumbent on us to overcome the misconception to think of computing as programming, a highly mechanical activity distinct from studies of the underlying theory and uses of the programming. Even a balanced study of (say) music is balanced by studies of the history of the field, case studies of successful implementations, the underlying theory and its application in various environments. Aficionados of a technology have a tendency to immerse themselves in the topic for its own sake. Studies which lead to an appreciation of ethical behavior must include an comprehension of the building blocks of the field (and an understanding of the pitfalls that were circumvented), the impact of the technology on not only the field but also its surrounding community, and the means by which this technology supports and fosters change in allied activities. Another paper can serve to justify the teaching of computer science as a range of interconnected topics where the learner will enter a career that has ramifications beyond his/her immediate environment. The purpose of computing in a secondary school or a university must be to teach/learn responsible, and yet enjoyable, problem solving, not just programming.

From these thoughts and from several years of a mission to bring an understanding of ethical notions to computer science students, I propose that the curriculum for computer studies must include the following themes (exemplified by some suggested subtopics):

(1) A study of the history of computing and its impact on society
- the pre-history and history of computing
- computer pioneers and their influence
- influence of computers on every day life
- embedded computer systems and communications
- the impact of computers on careers and jobs

(2) Case studies of the application of computers outside of computing itself
- computers in medicine
- computers and the military
- computers in business

---

[11] During a seminar that I conducted for 35 Savings and Loans Company managers, I inquired how many did the same kind of background checks on their programmers as they did for their tellers. Only three claimed to run background checks!

- artificial intelligence

(3) An understanding of the basis for ethics - codes of practice, intellectual property laws

- ethical theory - the difference between morals and ethics
- ACM, IEEE, DPMA codes of professional practice
- copyrights, patents and trademarks
- computer abuse laws

(4) Case studies, scenarios for ethical review

- ethical parallels
- hacking and computer misuse
- viruses, Trojan horses, trap doors
- computer crime
- daily ethical considerations

All of these elements need not be included in a single course, but where they are distributed over a collection of courses a coordination of the presentations be provided is imperative. Too easily the presentation of material from "modules", taken from an apparently disparate topic to that of the course, can be replaced by "make-up" inquiries from the major topic, or even may be forgotten when the teacher is uneasy in presenting material which outside of his/her area of expertise.

Conclusion

In discussing hackers and the melanoma alleged to be associated with their activities, we have perhaps overlooked the ultimate instantiation of their trade - the computer criminal. Clearly the computer is a tool that can be used in illegitimate manners just as almost any other tool in our modern repertoire can be used inappropriately. While much of the alleged activity of hackers has come under scrutiny in the legislatures, a line still exists between the hacker and the criminal. This line may hinge on intent and purpose, and while it is not clear that hackers accrue a great deal of financial benefit by their actions, the impact on the owner of a (hardware or software) system is not that different. Consider the disparity between the hacker ethic that information should be free and the right to privacy of individuals whose records are stored in a data bank. Fundamentally the system owner must rely on three elements that will provide his protection:

Computer Security - the technical means by which the system is protected by layers of security through which control of communication is verified and by which data and software is checked for sanity, cleanliness and appropriateness

Computer Law - the enactment of a series of punitive measures which define precisely the illegitimate activities with respect to computer systems usage, and the installation of an enforcement mechanism by which infringements of the law are detected and prosecuted

Computer Ethics - the introduction of studies of ethical behavior into our educational system, in the same manner in which ethical (and moral) behavior is studied alongside other topics which require personal ethical control

Security and protection are commonly taught in computer science curriculum at the university level and computer service organizations must divert computer cycles that would otherwise be available to users to protect systems against outside intrusion. Computer law is only now receiving attention in state legislatures and the national congresses; in any case laws tend only to keep honest people honest! Our least expensive and possibly the most effective counter to future computer and communications misuse is education. The time has come to include ethical considerations into computer curriculum, preferably at the secondary school level, with reinforcement at the college and professional school level.

Acknowledgements

Reading over one's own words is always difficult since one knows what was meant before you even read it again. My many thanks to Dr. Richard E. Nance, Virginia Tech, for his careful and thoughtful suggestions for improvement in the readability of this paper.

References

ACM. 1989. "The Worm Story", A collection of papers and reports, *Comm. ACM*, Vol. 32, No. 6, pp. 677-703.

David, E. E., Jr., and Robert M. Fano. 1965. "Some Thoughts about the Social Implications of Accessible Computing", in AFIPS, *Proc. Fall Joint Computer Conf.*, Vol. 27, Spartan Books Inc, Washington DC, pp. 243-247.

Dorsey, Gary. 1990. The Fullness of Wings: The Making of a New Daedalus, Viking, New York, esp. chapter 3.

Irwin, Stephen T. 1990. "The Great Hacker Challenge of 1989", *Technical Support*,..

Johnson, Deborah G. and John W. Snapper. 1985. Ethical Issues in the Use of Computers, Wadsworth Pub. Co.

Lee, J.A.N., Roz Steier, and Gerald Segal. 1986. "Positive Alternatives: A Report of an ACM Panel on Hacking", *Comm. ACM*, Vol.29, No.4, April 1986, pp.297-299.

Levy, Steven. 1984. Hackers: Heroes of the Computer Revolution, Anchor Press/Doubleday, Garden City, NY, 458 pp.

Robinett, Jane. 1991. "Ethics in Invisible Communities: Looking for Network Security in Our Changing Society", *Computer Research News*, Washington DC, Vol. 3, No. 1, p. 16.

Shapiro, Norman Z. and Robert H. Anderson. 1985. Towards an Ethics and Etiquette for Electronic Mail, Rep. No. R-3283-NSF/RC, Rand Corp., Santa Monica CA.

Joyce, E. J. Oct. 3, 1986. "Malfunction 54: Unravelling Deadly Medical Mystery of Computerized Accelerator Gone Awry", *American Medical News*, 1,pp.13-17.

Additional Suggested Reading:

Gemignani, Michael. 1989. "Viruses and Criminal Law", Legally Speaking, *Comm. ACM*, Vol. 32, No. 6, pp. 669-671.

Jennings, Karla. 1990. The Devouring Fungus: Tales of the Computer Age, W.W. Norton & Co., Inc., New York.

Landreth, Bill. 1985. Out of the Inner Circle: A Hacker's Guide to Computer Security, Microsoft Press, Bellvue WA, 230 pp.

Parker, Donn B. 1976. Crime by Computer, Scribner's, New York.

Parker, Donn B. 1983. Fighting Computer Crime, Scribner's, New York.

Parker, Donn, and John F. Maxfield. 1985. "The Nature and Extent of Electronic Computer Intrusion", Workshop on Protection of Computer Systems and Software, National Science Foundation.

Perry, Tekla S. and Paul Wallich. May 1984. "Can Computer Crime be Stopped?", IEEE *Spectrum*.

Samuelson, Pamela. 1989. "Can Hackers be Sued for Damages Caused by Computer Viruses?", Legally Speaking, *Comm. ACM*, Vol. 32, No. 6, pp. 666-669.

Steele, Jr., Guy L. et al. 1983. The Hacker's Dictionary, Harper & Row, Publ., New York.

Stoll, Cliff. 1989. The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage, Simon and Shuster Inc., New York.