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 general community has brought under its influence a number of individuals who may not be 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 leads 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

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

Good judgment comes from experience;
experience comes from bad judgment
- Jim Horning

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 only anecdotal evidence 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 teaches facts and skills, and from there, in the classroom community, develops interpersonal relationships leading to the need for decision making based on morals and ethics. However, unlike sex and driver education no claim can be made that computer education can also be accomplished effectively in the home as well as the schoolroom. Dissimilar from either of those other activities, few parents have adolescent computer 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"!*

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. The prevailing societal attitude is to get away with what you can. 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.

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. 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 not to 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 that may be included in early computer related courses.

The Risks

With the appearance 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.

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.

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

The Teenage Creed and Need

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

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[4]:

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 USA worried in 1918 about *"how are we going keep them down on the farm?"* - referring to GI's whose minds had been stretched by "Gay 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. 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. Goals and achievement levels within organized 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.

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. 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 those many users, having once been titillated by that "freebie", obtained updated versions illegally.

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?"*

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!

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. 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

With the joining of computers and communication came what we might term The Heisenberg effect of network communication. When computers appeared in personal offices, laboratories and even in homes, no-one was standing in line 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. 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. Security can be implemented by various means; shielded hardware and regulatory software are among the most common safeguards. 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!

next