Hacker values and a dilemma for information technology educators

BY NICHOLAS CHANTLER
Faculty of Law, QUT Brisbane

THE DILEMMA
Information-technology students are taught to be creative, to focus on a goal, to achieve, to use the computer as a tool to problem solve. We inspire them, we show them how to use their imagination and we encourage them to be creative. By giving them an insight into what the computer can do, we are unlocking, for some, what I believe is pure genius. The problem is that we cannot control on what we have unlocked. This is particularly vivid in extreme cases.

Do we put a student on the head for having cracked the code, hacking into a remote database, removing the software protection, as a result of using their imagination, focussing on a problem, drawing on resources, deciding on the right approach. They aren’t these the attributes in education that we are trying to promote? verses problem solving, self-direction in education, stimulating the minds of students and developing individuals into becoming motivated to the degree of being self-starters.

But how do we control their ethical behaviour? Can it be possible to only half-inspire them?

Perhaps the work of Dr. R. A. Coldwell (personal communication, 1990; 1992) can give us a clue in his comparison of attitudes between Arts and Science students. After being asked how they would feel if they learned that a hacker had accessed information about them in a restricted database. The Science students responses were of the ilk ‘great stuff, cool, good hack’ whereas the Arts students responses were ‘call the police! Send in the Army! We’ll get them’!

If we reflect on ourselves as information technology educators, how do we feel about a good hack? Do we have dual standards, and if we do, perhaps we don’t realise it? Is it a case of ‘do as I say and not as I do’?

HAVER VALUES
I have previously described (Chantler, 1992) a distinct pattern or model which evolves with those computer enthusiasts who are self-starters. I refer to the class of info-tech students who are known as ‘Computer Hackers, Cyberspace Junkies, Feral Whiz-Kids, Phreakers’, etc... or perhaps just ‘highly motivated techno-geniuses’.

They show resourcefulness, lateral thought, imagination along with the efficient and effective use of data.

Webster’s Dictionary defines Ethics as ‘a set of moral principles or values.’ A set of values is what directs a person’s life, and any description of a persons ethics would have to revolve around their values. Thus, I consider that ethics and values are tightly linked. Rokeach (1973) defines a value as ‘an enduring belief that a specific mode of conduct or end-state existence is personally or socially preferable to an opposite or converse mode of conduct or end-state existence.’ Hitt states that it is important to realise that values are beliefs, they are not facts; and that values are enduring, they are not transient.

My own observations and research on the ‘computer underground’ show that hackers do share common beliefs and values, and hence ethical viewpoints throughout cyberspace.

It is also apparent that within any circle of hackers there is an ‘honour amongst thieves’ ethics. Some of the recurring comments which have emerged from my surveys are:

‘I value friendship of like-minded people.’
‘I value the confidence others place in me.’
‘I value the input of like-minded people.’
‘I value honouring my friends.’
‘I value being recognised by my friends for my successful exploits.’

Here we see values which form an inseparable part of ethics. The values in themselves are perfectly acceptable but what of their acts?

‘I don’t see it (hacking) as a crime because we are only dealing with electronic impulses, and besides nobody is getting physically hurt.’

‘Australia supports the underdog and I only go for big companies.’

‘Anything to do with money is only “ones and zeroes”.’

‘I’m sitting at home at my PC, so who am I hurting?’

‘I only hack for the challenge.’

‘School is boring and I get so much more of a challenge from hacking.’

‘All information in cyberspace is free to those who live in that world.’

How can we as educators control or shape ethics, when the values displayed by these students are quite acceptable?

Should we rely on the ethics and values which have been placed on students from their parents? If ‘ethics’ is such a personal subject, do we even have the right, as educators, to teach ethics?

CONCLUSION
The intensity which computer hackers apply themselves to a task (the self-learning process) can be astounding when compared with ‘normal’ students.

The focus of problem solving can become all-consuming, to the extent of becoming an addiction in some cases.

We need to introduce ethics into courses that deal with information technology in order to maintain a societal balance. Too often, we immerse ourselves into the subject and forget about the real world.

We should consider three aspects for our students and ourselves:

• ethics for education
• ethics in computing/information technology
• personal ethics

REFERENCES
