Topic 2

Rights and Wrongs

Contents

Learning Objectives

- **Awareness of the international codes and standards governing the profession**
- **Appreciation of the law as it relates to computing**
- **Understanding of methods for the rational resolution of ethical problems**

2.1 Introduction

A variety of instruments can be used to identify which practices are regarded as acceptable and which unacceptable. Depending on whether these instruments are framed as professional codes, industry standards or statute laws, the punitive measures for malpractice can vary considerably in their severity. In this topic we shall look at the ways in which the computing profession can be regulated.

Rules and regulations aside though, we all bring our own moral values and ethical principles to bear when considering the rights and wrongs of a particular course of action. When our values and principles form a major part of the justification for our actions it becomes imperative that we are able to articulate them clearly to others. This can be very difficult if we are not used to

doing so though. We shall examine methods which can assist us in applying our ethical standards and explaining them to others.

2.2 Codes and standards

Compliance with codes or standards is generally voluntary, rather than compulsory. Professional codes are accepted voluntarily when one joins a professional body and failure to comply with the codes will normally result in expulsion from the professional body at worst. Industry standards are guidelines which should be followed, and might be a requirement for membership of certain industry associations, but they are not obligatory.

2.2.1 Codes

All professional bodies have codes of conduct and/or practice. We examined the codes of the British Computer Society in the previous topic. Other codes with which you might already be acquainted include the Code of Ethics and Professional Conduct of the Association for Computing Machinery (ACM) and the Software Engineering Code of Ethics and Professional Practice of the Institute for Electrical and Electronics Engineers Computer Society (IEEE-CS) jointly with the ACM (Quinn 2005). Intellect promulgate an IT Supplier Code of Best Practice and even the International Standards Organisation (ISO) has a Code of Ethics.

The emphasis on professional bodies and the sanctions which they can impose on members who do not comply with their codes does not mean that non-members are in some way exempt from these codes. Because the bodies are recognised as representing their professions and work hard to publicise their codes, no practitioner can credibly claim ignorance of them, nor be forgiven because they happened not to be a member. Familiarity and compliance with these professional codes of conduct and practice is expected of all practitioners, whether members of the professional body or not.

Typically professional codes will require that the practitioner pays due heed to –

- Staying up to date in knowledge of their craft
- Developing the knowledge and careers of others for whom they are responsible
- Providing clients with the most appropriate solutions to their problems
- Providing clients with impartial advice
- The interests of the public as a whole

That last bullet point can cause more heart-ache and lost sleep than all of the others combined. It places a requirement on the practitioner to look at the bigger picture surrounding what they are doing and the possible side-effects of their actions or recommendations. Doing the best job one can for a client is relatively straight-forward but it is not always the case that what is best for a particular client is best for society at large.

2.2.2 Standards

Standards organisations lay down guidelines for all sorts of manufactures and services. It is expected that a practitioner will be aware of and comply with any national and international

standards pertinent to their work. Whilst the standards themselves are not enshrined in law they can play an important part in legal cases. A defence against a law suit for negligence, for instance, is unlikely to be upheld if the relevant standards have not been complied with in the work of the defendant.

Of greatest importance are those standards that have risen to international status. The International Standards Organisation (ISO) publishes a number of standards relevant to the IT profession. Two with which you should familiarise yourself are –

- ISO 9000 Quality Management and Quality Assurance
- ISO 17799 Information Security Management Systems

The former actually has a computerised certification process known as TickIT which was especially developed to assist the computer industry in becoming compliant. It is worth noting, however, that even international standards are not beyond criticism. ISO 9000 is a case in point here, for it has been roundly accused of inflexibility and consequently actually reducing quality in some circumstances (Seddon, 1997). Having said that, it would be a foolish person indeed who tried to use Seddon's arguments as a reason for not using ISO 9000 if they didn't employ any other quality management system instead.

2.3 Computer law

Compliance with statute laws is, of course, mandatory and failure to comply can result in fines or imprisonment. There will probably be many laws within the jurisdiction where you live or work that are relevant to the IT profession. Some will be applicable to a wide range of activities with no special treatment given to computing. Some will pre-date key developments in computer technology and might have been amended (possibly in an unsatisfactory way) to cope with these developments as they arose. Others will have been framed specifically to deal with issues which result from computer and communications technology.

In the following sections we shall briefly examine five broad categories of laws that impact on the IT practitioner. You should not expect to be able to handle your own legal affairs as a result of the instruction you receive on this course but it is important that you are able to recognise situations when you need to call upon the services of a professional lawyer.

2.3.1 Contracts and consumer protection

Contracts, torts (wrongs) and restitution form a class of laws which generally have a long history and are unlikely to make special reference to the IT industry. You should note, however, that contracts can sometimes be held to be unfair and therefore not binding on the signatories. Indemnity clauses, where a contract states that the supplier cannot be held responsible for death or injury resulting from their product or service, are most likely to fall into this category. Consumer law can also be brought to bear in cases where fitness for purpose or safety are called into question. Compensation payments when things go wrong can be enormous. You should always take the advice of a lawyer when drawing up or signing a contract.

2.3.2 Intellectual property

Intellectual Property Rights (IPR) have become a hot topic with the development of IT and the Internet. With two notable exceptions, there is really nothing special about the computing industry when considering IPR; computer hardware can be protected by patents like any other invention and computer software can be protected by copyright like any other recorded form of intellectual property. In some jurisdictions changes were required to legislation to cater for electronic, as opposed to printed, forms but that was a relatively simple amendment to make.

The reason IPR has become such a hot topic, of course, is that computer and communications technology make it so easy to copy other people's work and so difficult to identify where that copying has actually taken place. It's not the case that laws need to be changed, it's that they have become so difficult to enforce. From the point of view of the IT profession, the main concern is to ensure that reasonable measures are taken to protect the IPR of others – the IPR of IT developers doesn't require any special new laws to protect it.

But what of the two notable exceptions we mentioned earlier? Well, one concerns computer algorithms and the other relates to the "look and feel" of computer programs and they cause problems because there is no consensus on how to handle them.

For computer algorithms the controversy arises over whether they should be patentable. It is not possible to copyright a computer algorithm. On this there is consensus. It is possible to copyright a particular implementation of an algorithm – as long as there is scope for a diversity of such implementations – but the idea of the algorithm, its essence, is not appropriate for copyright protection. If a computer algorithm is regarded as an "invention", however, then it should be possible to protect it with a patent. On the other hand, if an algorithm is viewed as a mathematical method then it should be treated like any other "discoverable" thing and thus be excluded from being patented. The argument rages on, particularly between the USA, which takes the former view, and the European Union, which takes the latter. Both sides claim that their approach offers the greater benefits to society as a whole. You might like to try listing their respective benefits for yourself.

The issue of the "look and feel" of computer programs boils down to whether we need a new kind of intellectual property. Suppose you create a computer program with a particular screen display and a particular layout of buttons, menus, etc. Suppose now that somebody else creates another, totally different, program which mimics the "look and feel" of your program perfectly. Have they violated your intellectual property? Some major computer companies would say yes and they have taken other companies to court over it. Other people would say no and point to the fact that no such restriction exists on copying the "look" or "user interface" of any other product type. What is your view on this? Do we need a new type of design right to protect the look and feel of things or would this just force every new product to be incompatible with everything else?

2.3.3 Data protection

Data protection legislation is becoming very widespread. The three pillars of such legislation are necessity, accuracy and privacy. Whilst these three concepts are often wrapped up in a

larger number of data protection principles, the important protections which they enshrine are that personal data relating to individuals –

- Should only be held if necessary to the task in hand
- Must be maintained as accurately as possible
- Should not be disclosed to anybody else

This last requirement probably represents a historic first in that it imposes a legal imperative which can only be met with technological solutions. The non-disclosure aspect of data protection laws places a legal obligation on the holders of such information to implement a raft of security measures ranging from access control procedures to data encryption. In this day and age it would not be accepted that reasonable measures had been taken to prevent unauthorised disclosure if such security mechanisms were lacking.

2.3.4 Computer misuse

Computer misuse legislation comes in as many forms as there are forms of computer misuse. Unauthorised access and unauthorised modification of data are commonly made criminal offences under such legislation but they are rarely the crimes for which criminals are really investigated. Charges of unauthorised access and data modification are normally brought as part of a much larger case, such as fraud. These larger crimes are covered by conventional criminal law and the specific computer misuse elements tend to play a small part in the overall case. Penalties for computer misuse alone seem commonly to have been set to deter mischievous teenagers rather than career criminals.

There is an increasing number of voices arguing for legislation to criminalise computer based obscenity and defamation but there are global differences in cultural and political perspectives on what is acceptable in these areas so an international consensus is unlikely to be achieved for some time, if at all. This is not to say that you can ignore these issues though. Most jurisdictions have laws banning certain forms of material and you should make yourself aware of those that affect you.

2.3.5 Computer evidence

We end our examination of computers and the law with a word of warning about computer evidence. Crimes involving computer technology can often only be proved in a court of law by means of audit trails, access logs, etc. However, the justice system is all too well aware of the fact that evidence can be tampered with. What easier form of evidence is there to tamper with than a computer file? Files containing trails and logs are just as easy to edit as any other files. In order to preserve the chain of evidence contained in these files it is essential that they are not accessed or modified subsequent to a crime or they may not be usable as evidence. So if you think any computer for which you are responsible might have been used to perpetrate a crime think twice before looking at the log files with an editor – isolate the computer and call in the experts.

2.4 Ethical decision making

Computer ethics, or at least the publishing of books on the subject, became something of a boom industry in the last decade of the twentieth century. It is not hard to see why. The influence of computer technology on so many aspects of people's lives was advancing at an alarming rate. More alarming still, to the media anyway, was the apparent lack of morality of the young people destined to be the future of the profession. They were hacking into top secret facilities, creating computer viruses, spreading pornography. What they needed was a good dose of old fashioned ethics to set them straight. Hence all the new modules in computing degrees entitled "Computer Ethics" or something similar and thence all the books to support those modules.

We shall not insult you by trying to give you a moral code here. We trust that you have one already. What you might lack is the wherewithal to apply your moral values to the complex and confusing world which computer and communications technology have created and in which you now find yourself so thoroughly immersed. Perhaps you find even that suggestion somewhat patronising? If so, we apologise but one thing the author of this unit has identified is that computer professionals are not at their most articulate when discussing ethical issues and their ability to justify their actions often leaves a lot to be desired.

The twin aims of this section are to introduce you to some methods which can help you think through an ethical dilemma and to assist you in explaining your decisions in ways which indicate that you have, indeed, thought about their consequences for all concerned.

2.4.1 Moral systems

There are many moral systems. Best known amongst them are those espoused by the great world religions. If you are religious you should have no difficulty in writing down the fundamental moral tenets of your religion which guide the way you treat other individuals and the responsibilities you have towards the wider community. If you are not religious then your moral lights might not be so readily expressed in time-honoured phrases but now would be a good time to pin them down to words on paper. At this point most of the aforementioned ethics texts present a potted history of European moral philosophy from the ancient Greeks down to the nineteenth century. If you think Plato, Aristotle, Kant or Mill might help you, feel free to make use of them. See Quinn (2005) amongst others.

The important thing to remember about the statements you have written down is that they apply to, and in, everything you do. They do not belong in a separate "non-technological" part of your life. They are the axioms which will help you wrestle with ethical problems and which will enable you to explain your decisions to others. All too often technologists feel obliged to explain themselves in a dispassionate and technical fashion which only fuels the concerns of those who would rather see some evidence of basic humanity. This does not mean that you should get all emotional and irrational. Rational thought and argument, weighing things in the balance, remain essential. You still need to be able to say things like –

> *In coming to this decision I gave due consideration to the consequences for X but concluded that they would be less severe than the impact on Y for the following reasons ...*

but by stating the moral cases for considering X and Y in the first place, even though they might seem obvious to you, you can re-assure people who might find the technology and the technical arguments intimidating.

2.4.2 Stakeholders

Kallman and Grillo (1993) suggested a very useful approach to making ethical decisions - whether this be to determine the morality of somebody else's actions or to help determine an ethical course of action to follow yourself. Their approach is to list all of the stakeholders in the decision.

Anybody who might be affected, either positively or negatively, by the choice being made should be given proper consideration. Stakeholders are not always easy to identify - some are only affected very indirectly. It can be helpful to tabulate the options and the stakeholders, noting the effect of each option upon each stakeholder.

2.4.3 Ethical tests

Kallman and Grillo also produced a collection of useful tests which we extend slightly for presentation here -

The Golden Rule
Treat others as you would have them treat you.

Other Person's Shoes Test
Does what you are proposing treat others as you would have them treat you *if you were in their position rather than yours* (cf. The Golden Rule).

Legality Test
Is what you are proposing legal?

Smell Test
Does what you are proposing smell right?

Parent Test
Would you tell your parents what you are proposing?

Media Test
Would you be happy for the media to find out what you are proposing?

Market Test
Is your proposed course of action such a good thing that you could actually sell it?

Always identify the important stakeholders and the key facts of a situation. It can help to write them down. Clarify the options open to you. Apply as many tests to each option as you feel are appropriate and consider the impact on the various stakeholders. Do this and you are unlikely to be accused of not giving due consideration to the consequences of your decisions.

2.5 Assigned task

You should select one of the following two ethical dilemmas and write a 2000 word essay discussing what you would do in that situation and why. This essay should be submitted at your second tutorial meeting.

1. Screen Capture Program

You are to imagine that you have recently become a development manager, overseeing a number of programmers and analysts working in project teams.

Three weeks ago, whilst browsing through a directory of materials which you have inherited from your predecessor, you discovered an application that lets you capture and view a snapshot of any of the screens used by the staff for whom you are responsible. Tactful enquiries on your part over the following weeks reveal a number of facts -

- Nobody knows about the existence of the screen capturing program
- About a year ago there had been a problem with productivity when certain staff had devoted a not inconsiderable amount of their working time to solving puzzles which they circulated amongst each other via e-mail
- Your predecessor had, apparently coincidentally, caught many of the offenders with these puzzles open on their screens and had reprimanded them
- Puzzling then dropped off and productivity picked up
- Productivity seems to have declined again since your predecessor left

You must now decide what to do about the screen capturing program. Discuss the ethical issues involved and come to a reasoned decision which you can justify to others.

2. Carcinogenic Fertiliser Data

You are to imagine that, at some point in the not too distant future, you have taken up a position as a systems analyst with a major agro-chemical company. After an initial period of fairly trivial work your employers entrust you with the processing of confidential data concerning a very promising new fertiliser for wheat. This you regard as a great accolade; since you are aware of the tremendous importance your company places on secrecy. Indeed, only some six or seven people in the whole enterprise have access to the data you have been charged with handling.

Three years later you have progressed well within the company and have been given much responsibility. You have been amply rewarded by your employers for the many evenings and weekends which you have devoted to your work. You have married and now have two children as well as a large mortgage and two nice cars bought with a loan from the bank - your assets are all invested in your house.

Then, the following year, disaster strikes; mortgage rates shoot up, house prices plummet, your partner (whose income has been on a par with yours) loses his/her job and, in the course of

your work, you learn that the company has discovered that at least 70% of the people who have consumed the wheat grown with that promising fertiliser of four years ago have contracted cancer.

On questioning your supervisor of four years ago about the fertiliser you are informed that nobody outside the company is likely to discover the connection and you realise that the company is planning a cover-up. Anybody within the company who breathes a word about the scandal will be sought out and peremptorily dismissed.

You must now decide what to do about what you know. Discuss the ethical issues involved and come to a reasoned decision which you can justify to others.

2.6 End of topic test

<!-- IU
Please insert a multiple choice test here. The correct answers to each question are underlined.
-->

Q1. Which of the following is not a professional body –
a). Association for Computing Machinery
b). British Computer Society
c). Institute for Electrical and Electronics Engineers
d). International Standards Organisation

Q2. The computer-based ISO 9000 certification system is known as –
a). CrossOFF
b). LickIT
c). TickIT
d). TickOFF

Q3. The international security management standard is –
a). BS 5750
b). BS 7799
c). ISO 17799
d). ISO 9000

Q4. In law, a “tort” is a –
a). Duty
b). Right
c). Wig
d). Wrong

Q5. Screen displays with their accompanying button layouts, etc. are called –
a). Footprints
b). Look and feel
c). Look and learn
d). Stereotypes

Q6. Which of the following was NOT suggested as a pillar of data protection –
a). Accuracy
b). Longevity
c). Necessity
d). Privacy

Q7. The criminalisation of what is beginning to be talked about –
a). Computer games
b). Computer–based obscenity
c). Hacking
d). Unauthorised computer access

Q8. A chain of evidence can be broken by doing what to a log file –
a). Editing it
b). Opening it
c). Reading it
d). Selling it

Q9. Which of the following ancient Greek philosophers was mentioned –
a). Diogenes
b). Plato
c). Socrates
d). Zeno

Q10. Which of the following asserts that you should treat others as you would have them treat you –
a). Bronze Axiom
b). Golden Rule
c). Platinum Lemma
d). Silver Theorem

References

Quinn, M.J., 2005, *Ethics for the Information Age*. Addison Wesley.

Kallman, E.A. & Grillo, J.P., 1993, *Ethical Decision Making and Information Technology*. McGraw-Hill.

Seddon, J., 1997, *In Pursuit of Quality: The Case Against ISO 9000*. Oak Tree Press.