Chapter 1. Introduction to Computer Ethics

Table of Contents

1.1 Scenarios

A good place to start on this course is to look at the reasons why we should study it at all. To facilitate this, we look at a few scenarios. For each of these scenarios, you should write think about any questionable ethical issues about each scenario. At his point you may not be to answer them, but you might have your own opinion. Write this down as well you should revisit them after relevant section and see if your opinion has been affected.

Hopefully these typical ethical questions illustrates to you the diverse characters of ethical issues including, property rights, privacy, free speech and professional ethics. Is computer ethics different to those that came before. Partially, the answer is no since all fields have similar problems and issue. Partially, the answer is also yes, since there are issues specific to computers such as speed and programs etc.

1.1.1 Scenario 1: Should I copy software?

John invests a small amounts on the stock market. Last year he bought and successfully employed a software package to help him with his investments. Recently, he met Mary who was also interested in using the software. Mary borrowed the package, copied it and then returns it. Both vaguely knew that the software was proprietary but did not read up the details. Did John and Mary do anything wrong, if so what?

Something to consider:

- Should software package be lent?
- When is it justifiable to break the law? Bad law, inappropriate law or if the law is easy to break?

1.1.2 Scenario 2: Should a company data mine?

Inga sells hardware and software to over 100 000 customers per year. She has 10 years' experience. As part of the billing process she keeps information on customers. She buys and uses a data mining tool to derive useful information about her client's information such as zip codes, credit card numbers, ID numbers etc. Most of this information identifies groups and not individuals. She can then use the information to market her wares more efficiently. Is this ethical since customers did not give her the information for this purpose?

Note: What is data mining?

Data mining is a process of exploration and analysis of large quantities of data, by automatic or semi-automatic means. This is done in order to discover meaningful patterns and rules. In many cases, the data was not collected primarily for the purpose of Data Mining.

Something to consider:

- Should customer be notified?
- Is there a need for establishment of a policy? What should this policy looks like.
- Professional responsibility (professional Ethics): Do professionals have a responsibility to ensure computing serves humanity well?

1.1.3 Scenario 3: Freedom of Expression

In the US, a student JB posted sex fantasies on the Internet called Pamela's ordeal. The story was fictional, but JB named the main character, Pamela, after a REAL student. In it, he described the rape, torture and murder of Pamela. He also exchanged e-mails with other people in the newsgroups, discussing sex acts. An alumnus saw this and reported it to the University. JB was then arrested and held in custody. He was charged with transmitting interstate communication of threat to injure another person. The charges were eventually dropped, but did JB really do anything wrong?

Something to consider:

- Should self-censorship be enforced. Who decides what is acceptable?
- Is there a need for a public policy?

1.1.4 Scenario 4: Professional Responsibility

Mike works for a Software development company which develops computer games for children aged 8-14. The latest game that Mike worked on, uses inferential reasoning and allows players to choose different characters, primarily macho man and sexy woman. The game is used mainly by boys. Recently Mike attended a conference on gender and minorities, where he described the above. The conference delegates discussed the issue of lower participation of women in computing and how to make the industry more attractive to women.

Back at work, Mike realised that his production team is all male. Should he refuse to work on this team? Should he ask for the team to be reviewed? Will the game sell as well if different message was given? What is his responsibility?

Something to consider:

- Should software package be lent?
- When is it justifiable to break the law? Bad law, inappropriate law or if the law is easy to break?

1.2 New Possibilities

New technologies bring with them new possibilities for both good and bad applications. Of course, this is not limited to the field of computing.

Activity 1

Think about ethical issues that are involved in carrying out your job or day to day activity. Focus on those tasks which are non-computing related. Are they any ethical guidelines for doing your job or activity? How these ethical guidelines were developed over time, and are how often changes are made to them. What are the trigger of these changes if any?

1.2.1 New Possibilities in Computing

There is no doubt that computers and related information and communication technology have introduced new possibilities to many activities that we do. In some cases, they allow people to do things that they have been doing for years, but now in a different way. For example,

- Consumers are able to buy goods on and offline using computers. The nature of the goods might be different (eg abstract data) but the principal remain the same.
- Computers allows for individual to be track without their knowledge.
- Computers eliminates human contact, for better or for worse
- Computers give wide access to data and information

There are also other activities that were hard to do without computer such as data mining. It was so hard to do that it was not done. This accounts for the lack of policy concerning data mining.

What is it about computers that make the computer environment different? Factors that have been raised included:

- **Speed**: Computers are able to do things at exponentially faster rate than ever before. For example, data mining was only possible (or rather made economically viable) by the advent of computers
- **Storage and accessibility of data**: Vast amount of data can be stored and easily accessible for processing.
- **Concept of a program**: How should one treat a computer program. Is it property or an idea. Is it something to be copyrighted or patented. We will deal with this later in the module.
- **Breadth of Distribution**: Information technologies have present consumers with a new channel of distribution that is faster and as yet not as regulated internationally as traditional channels.

Activity 2

Can you think of other factors that make the computer and IT environment different to a more traditional non-computing medium? As new technologies are introduced new factors are arising every day. Think about relatively new technologies such as cellular communication or satellite tracking devices? Have they cause new ethical questions? For each technologies you can think of, try to work out what it is about the technology that cause those ethical questions.

1.2.2 Computers Used in Social context

Another area that we should be considering is the use of computers in social context. This includes the use of a large database for governmental agency such as home affairs (to keep birth, death, address etc), police or the judiciary (for criminal records, fine etc). These agencies have always kept records in paper form long before computers came along.

Activity 3: Government Databases

1. What is the implication of keeping large databases by government agencies, ethical or otherwise?

2. Does introduction of these database affect Free Speech? If so how?

3. Consider the rights of the individual. Should they be given rights of access to their own data or the ability to change incorrect data? Also consider the impact of incorrect data even if they are changed but not propagated in a timely fashion.

1.2.3 Moral and Legal Issues

There are often many points of view to consider when it comes to dealing ethical issues. A good solution walks a fine line in balancing all these factors. However, often another factor against policymakers is time. Often there is a policy vacuum because ethical frameworks and laws are lagging behind the innovation. Sometime it takes a considerable time for the ethical framework to be developed for an innovation as the technology itself evolves so quickly. A policy vacuum is most effectively filled by introduction of appropriate laws, but this takes time. Company or personal policies or social conventions can often filled effectively filled the gap, while at the same time provide a starting point to framework creation and eventually laws.

1.3 Definitions of Computer Ethics

1.3.1 James Moor

The operation of computer systems and their associated communications systems are central to the economies of the developed world. The social impact of this technology has been immense, changing the environment in which computers are used, and in doing so giving rise to questions of right and wrong. Moor defines computer ethics as:

> *'.... The analysis of the nature and the social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology.'*

He uses the phrase 'computer technology' so as to take the subject matter of the field broadly to include computers and associated technology: including concerns about software as well as hardware and concerns about networks connecting computers as well as computers themselves.

1.3.2 Deborah Johnson

Johnson defines the study of computer ethics as

> *'The study of the ethical questions that arise as a consequence of the development and deployment of computers and computing technologies. It involves two activities. One is identifying and bringing into focus the issues and problems that fall within its scope, raising awareness of the ethical dimension of a particular situation. The second is providing an approach to these issues, a means of advancing our understanding of, and suggesting ways of reaching wise solutions to these problems.'*

1.4 Are Computer Ethical Issues Unique?

There have been many arguments that have been put forward to answer the question of whether or not computer ethical issues are unique? The answer to the question will imply a different way in which these issues can be dealt with. If they are not unique, an effective solution can be derived or adapted from what existing guidelines. If they are unique then a completely new way of dealing with them may have to be derived. Of course, there are also suggestions that the answer to the above questions is not as clear-cut. The different answers (and the reasons) includes:

- No, in the sense that there is nothing new under the sun. There has always been issues of privacy, property and freedom. The introduction of computers does not necessary introduce new way of doing things. Often computers increase efficiency but fundamentally, the way of doing the task is still the same.
- Yes, in the sense that a new technology has been introduced that never existed before. An example of this is the computer program. Computer programs are unlike anything that was preceded before it. It can be (and has been) regarded as properties like cars or houses, while alternative it can also be seen as an

individual expression, not unlike a song. Yet another alternative is to regarded as an idea.

- Yes, it facilitates new human actions that were not possible (or economically viable) before. For example, virus writing is a noticeable problem with computers. While it is arguable that similar problems existed prior to the existence computers, they were not of a large enough scale to be considered an ethical issue. Another example, that have been cited many times before involve the use of data mining.

While there are many answers to the question, it is clear that when an ethical issue arise, part of it may be analogous to existing framework, while part of it may be entirely new. It is the role of the policymakers to consider this question thoroughly before deciding on a solution. If the issues in question has an appropriate analogy, it could be employed as a starting point.

1.4.1 What Make Computer Ethics Different?

Moor (1985) claims that computer ethics is not like any other; it is described as a new area of ethics and as a unique kind of it. The arguments for such are based on the logical malleability of computers, the computer's impact on society and the invisibility factor.

The logical malleability of computers

Moor (1985) argues that what is revolutionary about computers is logical malleability. Computers are viewed as being logically malleable in that they can be shaped and molded to do any activity that can be characterised in terms of inputs, outputs and connecting logical operations. The logic of computers can be shaped in infinite ways through changes in hardware and software.

> *'Just, as the power of a steam engine was the raw resource of the Industrial Revolution so the logic of a computer is a raw resource of the Information Revolution. Because the logic applies everywhere, the potential applications of computer technology appear limitless. The computer is the nearest thing we have to a universal tool. Indeed, the limits of computers are largely the limits of our own creativity.'*
>
> Moor defines the driving question of the Information Revolution as *'How can we mould the logic of computers to better serve our purposes?'*

The computer's impact on society

As computer technology encompass more and more of our society, Moor sees more and more of the transforming effect of computers on our basic institutions and practices. Although nobody can know for sure how our computerised society will look fifty years from now, Moor argues that it is reasonable to think that various aspects of our daily work will be transformed.

> *'Computers have been used for years by businesses to expedite routine work, such as calculating payrolls. However, as personal computers become widespread and allow executives to work at home, and as robots do more and more factory work, the emerging question will not be merely "How well do computers help us work?" but "What is the nature of this work?"'*

The invisibility factor

An important fact about computers is that most of the time and under most conditions computer operations are invisible. Moor (1985) mentions three kinds of invisibility that can have ethical significance. The first variety of the invisibility factor is invisible abuse. James Moor defines invisible abuse as *"the intentional use of the invisible operations of a computer to engage in unethical conduct."* Moor suggests that a classic example of this is the case of a programmer who realised that he could steal excess interest from a bank.

> *'When interest on a bank account is calculated, there is often a fraction of a cent left over after rounding off. This programmer instructed a computer to deposit these fractions of a cent to his own account.'*

Although Moor views this as an ordinary case of stealing, he sees this pertaining to computer ethics because computer technology has provided the opportunity for such activities to go more often than not unnoticed.

Another possibility for invisible abuse is invasion of the property and privacy of others. For example, Moor identifies how a computer can be programmed to contact another computer over phone lines and *'Surreptitiously remove or alter confidential information'.*

Another example of invisible abuse is the use of computers for surveillance. Classic examples of such use are computerised employee monitoring and Closed Circuit Television (CCTV) technologies.

The second variety of the invisibility factor is the presence of invisible programming values, those values that are embedded into a computer program. Moor draws an analogy between writing a computer program and building a house.

> *'No matter how detailed the specifications may be, a builder must make numerous decisions about matters not specified in order to construct the house. Different houses are compatible with a given set of specifications. Similarly, a request for a computer program is made at a level of abstraction usually far removed from the details of the actual programming language. In order to implement a program, which satisfies the specification, a programmer makes some value judgements about what is important and what is not. These values become embedded in the final product and may be invisible to someone who runs the program.'*

The third and final variety of the invisibility factor is the invisible complex calculation. Moor argues that *"Computers today are capable of enormous calculations beyond human comprehension. Even if a program is understood, it does not follow that the respective calculations are understood. Computers today perform and, certainly, super computers in the future will perform, calculations, which are too complex for human inspection and understanding."*

Moor argues that the issue is how much we should trust a computer's invisible calculation. This becomes a significant issue as the consequences grow in importance. He illustrates this with an example:

> *'Computers are used by the military in making decisions about launching nuclear weapons. On the one hand, computers are fallible and there may not be time to confirm their assessment of the situation. On the other hand, making decisions about launching nuclear weapons without using computers may be even more fallible and more dangerous. What should be our policy about trusting invisible calculations?'*

1.4.2 Similarities of Computer Ethics to Other Ethics

The computer ethicist Gotterbarn in (Johnson, 1995) argues that the issues invoked by computers are not new or unique. Historically, there are many devices that have had a significant impact on society. Gotterbarn cites the example of the printing press, for which he argues that *We did not develop a new or unique ethics called printing press ethics'.*

He further argues that the flexibility of the computer is due to the *'Underlying strengths of the logical and mathematical capabilities implemented in the computer. The underlying flexibility of math and logic is greater than that of the computer, but we did not develop logic ethics and mathematics ethics.'*

The newness claim, argues Gotterbarn, *"Leads people to think that computer ethics has not yet found its primary ethical standard; so the discussion of computer ethics is not yet directed by any 'guiding principle' from which we can reason. This is different from our understanding of the older more established professions. Medicine, for example, is viewed as having a primary ethical principle - prevent death - which physicians can use to guide their reasoning."*

Journalism is viewed as having a primary ethical principle - report the truth - which journalists can use to guide their reasoning. The inference from the newness claim is *'That we cannot make ethical decisions in computer ethics because we have not yet found a primary ethical principal.'*

Gotterbarn argues that the uniqueness claim is even more dangerous: *'It leads one to think that not only are the ethical standards undiscovered, but the model of ethical reasoning itself is yet to be discovered; that is, even if we find a primary principle, we will not know how to reason from it.'*

Gotterbarn concludes that *'We have mistakenly understood computer ethics as different from other professional ethics. When we look at medical ethics, legal ethics, journalistic ethics, we have to distinguish the practitioners of those ethics from the ethical principles they affirm. The three professionals work in different* *contexts: medicine, law and journalism. However, when we talk of their professional ethics we do not consider them three different kinds. The distinguishing characteristics among professional ethics, is the context in which they are applied. Because there are three contexts, it does not follow that there are three distinct sets of ethical rules or three different kinds of moral reasoning. Nor does it follow that computer ethics is another unique set of ethical principles which is yet to be discovered.'*

Spinello (1995) is another computer ethicist who argues that the issues invoked by computers are not new or unique. He states that it would be a mistake *'To consider the ethics of computer technology as unique, separate from general business and social ethics.'* His premise is that these *'Revolutionary problems can be confronted with the same analytical tools and ethical categories used for more traditional concerns. It will be illuminating to regard these new dilemmas from the perspective of rights or duties or maximisation of consequences.'* He argues that our *'ethical tradition'* is rich enough to provide ample background for the thoughtful and comprehensive treatment of these new problem areas. However, it may be necessary to *'Revise our definition of certain rights such as privacy in light of the new realities created by the phenomenon of digital disclosure. Although we need to reinterpret what the right to privacy means on the frontiers of cyberspace, it is important to underline that the notion of a right to privacy, a right to control of information about oneself, has not lost its intelligibility.'*

1.5 Traditionalist Approach to Resolving Ethical Issues

A way of dealing with new ethical issues is to take a traditionalist approach. This involves identifying a moral norm and principles on which the issue is based, then apply them to the new situation.

For example, we can extend or adapt property law of ownerships such as copyright, patent and trade secrecy to that of computer software.

Activity 4

E-mail is another technology that has an equivalence that one can consider applying the traditionalist approach on.

1. Identify the issues that might be of concern to e-mails include confidentiality (communication is private) and authentication (sender is who he or she claim to be).

2. How does traditional snail-mail deal with such issues? Are there any issues that does not have a snail-mail equivalence? Concerning these issues, what is it about e-mail that make it differ from snail-mail? (If you cannot think of anything, you can also start by first identifying the difference between e-mail and snail-mail, and then go on to say how each factors can raise new issues that were not applicable to snail-mails)

There are also problems with employing the traditionalist approach. This approach can result in oversimplification of issues, as it implies a routine way of dealing with ALL problems. The computing process is fluid with technology over changing.

Another issue is that different people will employ different analogies which can lead to different solutions. For example, the Internet can be thought of as a network of highways as well as a shopping mall. Choosing which analogies to used may lead to unsuitable solutions to some of those involved. How should computer program be considered? Is it property, idea or something else?

Activity 5: Analogy for Hacking

Compare and contrast the different between a hacker breaking into a computer system and a thief breaking in to a house. Is this a reasonable comparison? Is it a good analogy to employ while considering the issue of hacking?

Consider a scenario where a person walks down a street trying each door. If he founds and unlocked door he goes in and looks around. Is this situation analogous to a hacker scanning ports on a computer and find an opened port and goes in a look around and take a few things. However, also consider that in computer terms, some ports are considered public ports (for example, port 80 where web pages are served from). For example, is it reasonable to assume that if port 80 is available, the owner of the site gives you permission to access the site.

How far can you take this argument. For example, if a wireless signal is available, could you derived from that the owner gives you permission to access it? In some culture, a public water well or tap, is considered to be freely available to all that come passed. Should publicly accessible wireless signal then falls under the same category?

Chapter 2. Philosophical Ethics

Table of Contents

2.1 Theoretical Frameworks

According to Spinello (1995) the purpose of ethics is to help us behave honourably and attain those basic goods that make us more fully human. Ethics of this type, often called normative ethics, is distinct from the discipline of metaethics. Spinello defines metaethics as *'The study of moral discourse, the meaning of ethical terminology, and provability of ethical judgements. It deliberately eschews the old Socratic questions that are also asked by Aristotle: "How should life be lived?" or "What is the good life?"'*

Normative ethical inquiry, on the other hand, is a quest *'For the practical truth of how one's choices and actions will be good and worthwhile.'* Thus Spinello concludes: *'Whereas the goal of metaethics is an appreciation of the structure of moral language, the goal of normative ethics is an identification of the true human good.'*

Hence, normative ethical inquiry seeks a basis for choosing proper actions and the right way of life. However, ethics is not an exact science and therefore the same levels of objective truth that is possible in the rational sciences or mathematics cannot be attained. But the fact that ethical judgements do not have the same deductivity and objectivity as scientific ones does not imply that ethics consists merely of emotional and subjective opinions. Moral judgements should be based upon rational moral principles and sound, carefully reasoned arguments. Normative claims are supported by *'An appeal to defensible moral principles, which become manifest through rational discourse.'*

Also, simply because there is no unique, correct solution to a moral dilemma, it does not follow that all solutions are equally valid. A moral position can be assessed according to objective criteria, in terms of whether they respect or violate basic *'Human rights, remain open to human fulfilment, maximise the social good, etc.'* and therefore these criteria disqualify some solutions to ethical dilemmas in favour of others. Some basic moral principles and theories that can serve as normative guidelines for addressing the ethical issues invoked by computers will be considered later in the chapter. These guidelines constitute a framework for the ethical analysis of cases where ethical and professional issues may have been invoked. The initial step in conducting an ethical analysis is to establish one or more issues to be analysed. Then for each issue the law and principles presented in each of the four processes of the framework are applied. For each issue one or more alternative options are often highlighted. The analysis will disqualify some options to the ethical issue in favour of others. The intention of an analysis is to present these alternative options to a user and allow them to rationally examine these and choose the correct one.

The normative guidelines described below are those that appear in the Kallman and Grillo (1996) framework.

> *However, the danger of making an appeal to as many ethical principles as possible is that sometimes they conflict. In analysing an action, the course of action that is suggested by one ethical philosophy might contradict the course of action that is suggested by another. For example, Egoism focuses on self-interest. This ethical principle is used as justification when something is done to further an individual's own welfare. The principle of Utilitarianism embodies the notion of operating in the public interest rather than for personal benefit. However, an appreciation of ethics allows individuals to be aware of all possible ethical resolutions and their respective implications. An appropriate course of action for an individual should only be arrived at after thinking through all the implications. The intention behind an ethical analysis should not be to prescribe a particular set of ethical values for resolving ethical issues invoked by computers. But allow an individual to appreciate all the possible course(s) of action that can be taken according to the differing, and often conflicting, sets of ethical values and then make a judgement as to which is applicable for them in the real world.*

2.2 A Framework for Ethical Analysis

The first task is to list all the relevant facts. The stating of facts is, as suggested by Kallman and Grillo *'As much as possible, a neutral, logical exercise'.* Although interpretation is involved in selecting pertinent facts, they are not judged in this step.

The second task is to list the stakeholders in the case to determine who is affected by the action being analysed. A judgement must be made as to whether a stakeholder is important enough to be listed. There may also be a number of secondary stakeholders, and including them and their claims might not improve the depth of the case analysis.

Finally, it is necessary to consider the course of action the stakeholders have or are considering taking. This is achieved by asking whether they were or are under an obligation or duty to have done or not have done something. In addition, it is important to evaluate all the reasons that individuals give or may give to justify their actions, i.e. failing to fulfil their duty. One way to do this is to ask the question 'Does it matter....?' and then consider each of the reasons given in turn to determine which failings are significant and which are trivial.

Having established one or more of the courses of actions for each stakeholder, the principles pertaining to the following four steps (presented in sections 3.1-3.4 respectively) should be applied: Formal Guidelines, Ethical Theory, Legal Issues and Informal Guidelines.

2.2.1 Formal Guidelines

Areas addressed by professional codes are areas of concern in computer ethics, and the professional codes provide guidance related to making ethical decisions. A professional code is a set of rules that state principal duties all professionals should endeavour to discharge in pursuing their professional lives.

Consult corporate or professional codes of conduct

The first principle under Formal Guidelines is to consult corporate or professional codes of conduct. Since reference to a specific code may be a shortcoming because it fails to take into consideration cultural differences, the guidelines referenced should be as universal as possible. The computer ethicists Martin and Martin made a comparison of the ethical codes of four computer societies:

1. Association for Computing Machinery (ACM)

2. Institute of Electrical and Electronics Engineers (IEEE)
3. Data Processing Managers Association (DPMA) and
4. Institute for the Certification of Computer Professionals (ICCP)

They found ten common themes that emerged as the core for ethical behaviour for computer professionals:

1. Personal integrity/claim of competence
2. Personal responsibility for work
3. Responsibility to employer/client
4. Responsibility to profession
5. Confidentiality of information
6. Conflict of interest
7. Dignity/worth of people
8. Public safety, health, and welfare
9. Participation in professional societies
10. Increasing public knowledge about technology

These ten universal common themes are referenced in an ethical analysis.

The second principle to be referenced under Formal Guidelines is extracted from Confucianism. Confucianism is the ethical system of the Chinese philosopher Confucius (551-479 BC). Confucius's ethical system is sometimes summed up in the rule:

> *'What you do not want others to do to you, do not do to them.'*

In ethics this is known as the Golden Rule.

Having highlighted the course of actions that stakeholders have or are considering taking, the ten universal common themes and the Golden Rule should be applied to determine whether the consequences of these actions are ethical or unethical. If a specific course of action committed by a stakeholder fails to fulfil any of these principles given in this section then the action can be defined as unethical.

2.3 Ethical Theory

The modern ethical theories Deontology and Teleology are considered.

2.3.1 Deontology

According to a deontological framework, actions are essentially right or wrong regardless of the consequences they produce. An ethical action might be deduced from a duty (pluralism) or a basic human right (contractarianism) but it never depends on its projected outcome.

Duty-based Ethics (Pluralism)

According to WD Ross in (Kallman and Grillo, 1996) there are seven basic moral duties that are binding on moral agents:

1. One ought to keep promises (fidelity)

2. One ought to right the wrongs that one has inflicted on others (reparation)
3. One ought to distribute goods justly (justice)
4. One ought to improve the lot of others with respect to virtue, intelligence, and happiness (beneficence)
5. One ought to improve oneself with respect to virtue and intelligence (self-improvement)
6. One ought to exhibit gratitude when appropriate (gratitude)
7. One ought to avoid injury to others (non- injury)

Rights-based Ethics (Contractarianism)

Focuses on moral principle instead of consequences. A right can be defined as entitlement to something. In the field of Information Technology, Ernest Kallman identified three specific rights:

1. The right to know
2. The right to privacy
3. The right to property

2.3.2 Teleology

Teleological theories give priority to the good over the right, and they evaluate actions by the goal or consequences that they achieve. Thus, correct actions are those that produce the most good or optimise the consequences of choices, whereas wrong actions are those that do not contribute to the good. Three examples of the Teleological approach to ethics are Egoism, Utilitarianism and Altruism.

Egoism

Egoism focuses on self-interest. This ethical principle is used as justification when something is done to further an individual's own welfare. Asking the following question can best sum up the principle: 'Does the action benefit me, as an individual, in any way?'

Utilitarianism

The principle of Utilitarianism embodies the notion of operating in the public interest rather than for personal benefit. The principle extracted from this theory determines an action to be right if it maximises benefits over costs for all involved, everyone counting equal.

Altruism

> *'Is invoked when a decision results in benefit for others, even at a cost to some'.*

The principle extracted from this theory determines an action to be right if it maximises the benefits of some, even at the cost to others involved. In addition, the normative principles of Nonmaleficence, Autonomy and Informed Consent are also considered. On account of their simplicity and concreteness, Spinello sees these principles as serving *'A more practical and direct way of coming to terms with a moral dilemma'.*

2.4 Normative Principles

2.4.1 The Principle of Nonmaleficence

The principle is best summed up in the simple phrase, *'above all do no harm'*. According to this most basic of all moral principles, needless injury to others ought to be avoided whenever possible. The academic Gunneman states:

> *'We know of no societies, from the literature of anthropology or comparative ethics, whose moral codes do not contain some injunction against harming others. The specific notion of harm or social injury may vary, as well as the mode of correction and restitution but the injunctions are present.'*

2.4.2 The Principle of Autonomy

Kant and other philosophers have stressed that a vital element of person hood is the capacity to be self- determining. The Kantian notion of person hood emphasises the *'Equal worth and universal dignity of all persons, because all rational persons have a dual capacity: the ability to develop a rational plan to pursue their conception of the good life, and also the ability to respect this same capacity of self- determination in others. In other words, for an individual to be truly human, that person must befree to decide what is in his or her best interest.'*

2.4.3 The Principle of Informed Consent

The principle implies that someone has given agreement freely to something. For such an assent to have significance, it should be **informed**, that is, based on accurate information and an understanding of the issues at hand. If this information is deliberately withheld or is incomplete because of carelessness, then the consent is given under false pretences and is invalid.

Referring to the highlighted course of actions that stakeholders have or are considering taking, the ethical principles stated under deontology, teleology and the normative principles should be applied to determine whether the consequences of these actions are ethical or unethical. However, it is important to note that in analysing any specific course of action, the evaluation of that action that is suggested by one ethical philosophy might contradict the evaluation of the same action by another ethical philosophy. For example, a moral duty to improve one self may conflict with a utilitarian duty to operate in the public interest. The principles are simply allowing you to assemble a rational reason for your course of action. A moral position for a course of action can be assessed according to objective criteria, in terms of whether they respect or violate the basic ethical principles presented in this section.

2.5 Law

When a law tells us to do or not to do something, it implies that a recognised, established authority has decided that the action the law permits or prohibits is of some benefit to society in some way. It often happens that an ethical principle was the basis for any decision regarding this issue before the law was constructed. The fact that the law is grounded in ethical principles makes law a good point for ethical decision making. In other words, Kallman and Grillo (1996) suggest

> *'That when we are confronted with an ethical decision, we should first research the law'.*

In some instances, the law will clearly apply and lead directly to the appropriate ethical conclusion. However, to rely solely on law as a moral guideline is clearly dangerous because as highlighted by Jennifer Wagner (1991) four possible states exist in the relationship between ethics and law. Wagner's taxonomy identifies four possible states which depend on whether a specific act is ethical or not ethical, and legal or not legal. The table below presents these states. This implies that in certain circumstances bad laws exist. Bad laws may bind rules on society that fail to provide moral guidance. Such laws may in some instances excuse a society from fulfilling certain obligations and duties, or allow a society to justify their unethical behaviour. However, beyond any doubt, law and morality do have in common certain key principles and obligations.

Legality versus Ethicality

	Legal	Not Legal
Ethical	I	II
Not Ethical	III	IV

- I = An act that is ethical and legal

- II = An act that is ethical but not legal
- III = An act that is not ethical but is legal
- IV = An act that is not ethical and not legal

Activity 1: Law and Ethics

Think of a scenario (need not be related to computing) that best illustrates each state that exists in the relationship between law and ethics.

You can find some discussion of this activity at the end of this chapter.

2.6 Informal Guidelines

The following tests allow for quick evaluation of a situation in an attempt to resolve an ethical dilemma Kallman and Grillo (1996) define these has informal guidelines.

2.6.1 Moral Intuition Test

The test involves asking the following question:

> *'Consider your first impressions or reactions to these issues. In other words, what does your moral intuition say about the action or policy under consideration: is it wrong or right?'*

The merit of using this principle is that, as in the other tests, it allows for quick evaluation of a situation in an attempt to resolve an ethical dilemma.

2.6.2 The Mother Test

Discovers simply whether the individual would be proud or ashamed of an action, whether they would tell their mother what they did. The test uses a highly personal reaction as the first indicator of a problem.

2.6.3 The TV Test

Attempts to determine how the individual would feel if they saw their situation described on TV, whether their action would make them appear good or bad. How would millions of TV viewers react? In this test you *'pretend your ethical dilemma is being publicised far and wide'*.

2.6.4 The Smell Test

Simply asks whether the situation *smells*. Does the individual *feel in their bones* that there is a problem, but cannot pin it down. Does the individual's instinct tell them that something is wrong?

2.6.5 The Other Person's Shoe Test

Discovers actions that violate the ethical concept of the public interest. It asks what if the roles were reversed? Would the individual be happy if the act were done to them? If the individual would not want the roles reversed, then there is probably something wrong.

2.6.6 The Market Test

Determines whether the individual would use their behaviour as a marketing tool. In other words, does the individual's action have enough merit to give them a marketing edge? Would publicising their action reap praise or criticism for their organisation? If the answer is criticism the action is deemed to be unethical.

2.7 A Defensible Choice

Ethical choices are not made with absolute certainty; they are not deductive like mathematical problems and solutions. Ethical decisions are made through judgement and by validation through a rational appeal to a number of principles, as above. There is no unique correct solution to a moral dilemma. However, in assessing moral positions, a person can rationally examine alternative options and choose the correct one. Chris Sadler concludes:

> *"You can make a rational choice - that means you can give reasons for your choice. But it can still be morally wrong or morally repugnant to somebody else, or just different to what somebody else would have done in those circumstances. . All you can do is make a decision that is 'right for you' and going through the guidelines helps you to find out what that is and also to assemble your reasons (i.e. rational basis) for doing it."*

The rules and principles presented in the above framework can be applied to the case facts of instances where ethical dilemmas have been invoked in the development and deployment of computers.\

2.8 Additional Principles

In addition to the normative principles given above, an individual can make a rational appeal to The Ten Commandments of Computer Ethics has advocated by Arlene Rinaldi's Netiquette Webpage:

1. Thou shalt not use a computer to harm other people
2. Thou shalt not interfere with other people's computer work
3. Thou shalt not snoop around in other people's computer files
4. Thou shalt not use a computer to steal
5. Thou shalt not use a computer to bear false witness
6. Thou shalt not copy or use proprietary software for which you have not paid for
7. Thou shalt not use other people's computer resources without authorisation or proper compensation
8. Thou shalt not appropriate other people's intellectual output
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow human being

To be ethical, an action should elicit a positive response to all applicable primary questions and a negative response to each clarification:

- Is it honourable? Is there anyone from whom you would like to hide the action?
- Is it honest? Does it violate any agreement, actual or implied, or otherwise betray a trust?
- Does it avoid the possibility of a conflict of interest? Are there other considerations that might bias your judgement?
- Is it within your area of competence? Is it possible that your best effort will not be adequate?
- Is it fair? Is it detrimental to the legitimate interests of others?
- Is it considerate? Will it violate confidentiality or privacy, or otherwise harm anyone or anything?
- Is it conservative? Does it unnecessarily squander time or other valuable resources?

2.9 Where do Personal Values come from?

Their family and workplace may affect a person's views, but there are other areas of influence. In fact the number of such possible influences is potentially huge. Human interaction is recursive, every aspect of the way in which individuals react with those around them in turn colours the way they perceive the world, and so modifies their interaction with it. Some of these influences that shape our personal value are: Family / friends; Colleagues; Workplace; Industry / profession; Community; Law; Religion; and Culture: includes media, arts.

2.10 MARXISM: When Economics Determines Everything, Even Morality

Everything that Karl Marx (1818-83) wrote and thought stemmed from his conviction that all human activity was economically determined. Marx believed that political activity - just like religion, culture and morality - took its form from the economic system that gave it birth. And through all the centuries of human history - especially under the economic system of Western Capitalism as it operated when he was writing, in the middle decades of the 19th century - one theme stood out: class warfare and the exploitation of one class by another.

He advocated three classes: the landed aristocracy; the bourgeoisie (capitalist employing class); and the proletariat (wage earning, employed class). Because each class held a unique position in the economic system this implied their respective religion, culture and morality differed accordingly.

Activity 2: Personal Values

Ask colleagues, family and friends to identify their personal values. Can you identify any personal beliefs that differ from the ones held by your colleagues, family and friends? List these differences. How do you believe these differences may have arisen? Can you identify any universal core beliefs that are held by everyone you know, that could possibly be held by every human?

2.11 Answers and Discussions

2.11.1 Discussions of Activity 1

An act that is ethical and legal: The act of non-discrimination on grounds of race, gender, disability, sexual orientation, etc. is ethical and via discriminatory legislation legal.

An act that is ethical but not legal: The act of euthanasia can be seen as ethical, yet in some countries such as the UK is illegal.

An act that is not ethical but is legal: Apartheid, segregation of blacks and whites in South African society, totally unethical yet was legal under white rule.

An act that is not ethical and not legal: Torture of political prisoners is unethical and illegal under UN Declaration of Human Rights.

Chapter 3. Professional Ethics

Table of Contents

3.1 Scenarios

3.1.1 Scenario 1: Safety Concerns

Carl works for general purpose software and hardware company on a project for the military. The project involves developing a system that monitors radar signals for missiles and launches nuclear missiles when deemed necessary. Carl was initially reluctant but eventually agrees. His thinking was that if he does not do it, someone else will anyway. During his work he develops some reservations concerning the fine distinction between missiles and small planes. He expresses this to his manager who promptly dismisses the claim on the basis that he does not agree with the claim and that the project was already late.

Carl feels morally responsible. What should he do? What can he do?

- Ask for reassignment
- Go higher up in his company with this concern
- Go to the contractor in this case, the military
- Go to the newspaper (whistle blow) – this will likely lead to him losing his job.

3.1.2 Scenario 2: How much Security?

LJ has a computer science degree and has three years work experience. She has her own company and one of the current projects involved designing an employee database for a large company. The database contains medical records, performance evaluation, salary etc. She must decide on the security required for this system. The question is how much security.

She believes that the client should have all the necessary information that the client can use to based their decision on. She then presents ALL available options to the clients, with the level of security proportional to the cost. The client chooses the cheapest and least secure option, which leads LJ to feel that this is insecure. She explains the risks to the client but they sticks with the cheapest option. Should LJ refuse to build the system? Should she have presented this option to the client in the first place?

3.1.3 Scenario 3: Conflict of Interest

Juan is a private consultant. His job is to evaluate automation needs and recommend suitable systems. Recently he was hired by a hospital to upgrade their systems. He recommended (with reasons) Tri- Star as a best system to upgrade to. However he failed to mention that he is a partner in Tri-Star and that there is a conflict of interest. Was his behaviour unethical? Should he have:

- Decline the job originally
- Disclosed his ties with Tri-star?

3.2 Why Professional Ethics?

The three scenarios illustrate difficult situations. To solve them we could use utilitarian or deontological theories but they are only useful if the contexts of the problem are taken into account – i.e. the fact that Carl is a professional and employee of a company and that LJ and is professional, owner of the company and has a contract with the client. In these situations, we must consider what it means to act as a professional. What responsibilities do:

- employees have to employers and vice versa
- professionals have to the client and vice versa

We must recognise that professional role is special because it carries special rights and responsibilities. Some occupational roles are said to be STRONGLY DIFFERENTIATED where by professionals are granted powers exceptional to ordinary morality (eg. Consider medical doctors). Most occupational roles are NOT strongly differentiated.

It is claimed by most that the computing profession is NOT strongly differentiated i.e. computer professionals do not acquire special power/privilege by virtue of being in the profession. However this is not always the case - when hired to do a job, professionals do acquire powers and hence obligations that come with them. For example, Carl has obligation to his company but does not do everything his boss asks. LJ has obligation to the client for the security that they want.

3.3 Characteristics of a Profession

At this point, we need to see if computing is indeed a profession. Before proceeding to that, we look at the characteristics of a profession.

1. Master of an esoteric body of knowledge: This is usually acquired by a higher degree. Often the discipline embraces a division between researchers and practitioners.

2. Autonomy: Members are autonomous in their work. They make decisions and NOT take orders from others. They regulate themselves and set their own admission standards. The also have standards of practice.

3. Formal Organisation: There is often ONE unifying organisation which is recognised by the State. This organisation:

   i. Controls admissions.
   ii. Accredits educational institution.
   iii. Sets up and administrates disciplinary procedures.
   iv. Has the power to expel members.

4. Code of Ethics: This sets standards of the organisation and is used to maintain its autonomy. Members must adhere to this irrespective of their employment contexts.

5. Social Function: A professional must been seen to fulfil some useful and important social functions.

3.4 System of Professions

Many groups wish to be considered professional. To achieve this status the group needs to bee organised into a formal unit. They must also demonstrate a domain of activity and that if the group has control over this domain that it will be safer and more effectively run. The group must convince the public that lay people can not adequately judge the group and that only the group themselves are capable of judging themselves. Usually professional monopolies are granted on conditions that they must regulate themselves and that they must further the interests of the public.

This means that a professional group must:

- Convince the public of their special knowledge.
- Show that important social functions are at stake.
- Convince the public to trust the group (usually by means of code of

Ethics) For success the group needs:

- Formal organisation to gives the group monopoly
- Collective autonomy in order to justify individual autonomy for members
- Self regulation

3.5 Is Computing a Profession?

The computing filed is young and very broad. This is in sharp contrast to the medical and accounting fields. It is also very malleable i.e. it is used in many domains teaching, engineering, librarians etc. Some of these workers are not seen as computer professionals.

So is computing a profession? We compare computing with the five characteristics of profession.

1. **Mastery of Esoteric Knowledge**: Many do acquire knowledge through higher educational institutions. This is more true as time goes on. There also exists a division between researchers and practitioners. There is a large demand as many in the field have inadequate knowledge. However, some people have argued that computing relies on how to do things and not on a systematic and abstract body of knowledge.

2. **Autonomy**: This is not strongly differentiated i.e. there are no jobs that only professionals can do that others can not. Although this could be considered a chicken/egg problem).

3. **Formal organisation**: There are many such organisations in many countries such as CSSA (Computing Society of South Africa) and the BCS (British Computing society).

4. **Code of ethics**: There is no single code worldwide but they do exist. CSSA has such a code.

5. **Fulfilment of a social function**: Computing is a crucial part of society, but does it fulfil a need. It supports a variety of social functions but is not one in itself.

3.1.4 Software Engineering

Software engineering (development of a computer system) might seem like a good area of computing for professionalism. Its activities involved unique knowledge, education, licensing of members and code of ethics. ACM and IEEE decided not to support it because it does not yet have an identifiable body of knowledge. However, this has been done in Texas - they created a society that runs licensing examinations. It helps to belong but is not essential i.e. one can get work without membership.

3.6 Professional Relationships

These relationships are employer-employee, client-professional, society-professional and professional-professional.

3.1.5 Employer - Employee Relationships

This often involved the conditions of employments. This can be explicit in the contracts (concerns responsibilities and salary) but many important issues are left out (overtime). Some are specified by laws such as sick and annual leaves, while some are negotiated by unions such as retrenchment rules.

Moral foundation for this relationship:

- Is contractual
- Individuals should be treated with respects and not merely as a means.
- Neither party should take advantage of the other. Employee should be honest with their qualification and employer should not exploit employee (decent wage, safe environment, etc.)

Another important issue is what does the employee owe?

- Loyalty – can invite some unfairness (boss's son) or loss of criticality (just agree with boss)
- Trade secrets/knowledge in a field. There are many means of dealing with this, by making sure that:
- Employee can only sell specific knowledge – but this is considered wrong.
- Employees sign contract not to reveal secrets gain during employment as part of the job.
- Employees sign contract not to work in similar area for a certain period after leaving the company.

3.1.6 Client – Professional Relationships

Recall Carl and his safety concern. His company should have told the military that the project was late. In this respect, his company was not acting well. Additionally Carl tried to work through his company but failed. The client (the military) depends on professional for the knowledge and expertise in the special area.

There are different models for this kind of relationships:

- Agency: Professional is the agent and does exactly what client tells him to do (like telling a stockbroker to buy "Telkom").
- Paternalistic: Professional makes all the decisions and the client abrogates all decision making.
- Fiduciary: Both parties play a role by working together. The professional offers options while the client decides which one to take. This requires trust on both sides and that the decision process is shared.

3.1.7 Society – Professional Relationship

This relationship is usually shaped by law, but the law (or people who makes them) can not foresee everything - consider Carl's case. If Society licenses a professional society then the professional society:

- Must serve the interests of Society in general.
- Certainly must not harm Society.

- Must maintain itself.
- Must take DUE CARE based on the special knowledge it processes.

3.1.8 Professional – Professional Relationships

Many believe that this relationship is self-serving. They see members as only having an obligation to other members. This might create a reluctance to criticise another professional. Often such scenarios are complex, especially when it is difficult to tell if it's a genuine errors or incompetence.

For a professional society to flourish there must also be advantages to Society from it:

- Members must consider what they owe to each other to maintain standards of conduct.
- There is a need for disciplinary hearing procedure.
- Members have important obligation such as much not take bribes, not lie about qualifications or fudge the results.

3.1.9 Conflicting Responsibilities

For a professional, there exist many conflicts between the four types of relationships that they take part in. This is most common between the responsibilities with employer and society. Consider the Carl's case again – the company needs contracts to survive but Carl's concern is his responsibilities to society. So when does a professional 'rock the boat' when it comes to society versus other relationships? There is no easy answer but generally:

- Professional must be convinced of their position.
- Must consult managers at different levels of their company first.
- If they whistle blow they must be prepared to lose their jobs.

Another issue is fragmentation. Whereas medical profession sees the entire problem, computing professionals often sees a small part of the system and as such it can be very difficult to pass judgement.

Chapter 4. Code of Ethics and Professional Conduct

Table of Contents

4.1 Introduction

A code of ethics is a statement of collective wisdom of the members of the profession that expresses experience and consensus of many members. The code itself has several roles:

- Serve the interests of the Public.
- Protects the Public.
- Promotes worthy practices.
- Statement of shared commitment of members of the profession.
- Statement of agreed values.
- Statement of agreed rules.
- Sensitises members to important issues.
- Mechanism for educating for those entering the profession, companies and clients.

The code also ensures collective responsibility, so that various parties do not only think of individuals in the profession but rather a collective unit of the profession. If a profession speaks out on an issue, it is more effective as a group. Examples of this are issues such as protection of whistle blowers and gender bias.

4.2 IIPTSA Code of Conduct

IITPSA, The Institute of Information Technology Professionals South Africa (http://www.iitpsa.org.za/), formerly

Computer Society South Africa (CSSA), is a South African Qualifications Authority (SAQA) recognised Professional Body for South Africa's professional community of ICT practitioners. IITPSA has a code of conduct – a guide on how to handle issues. It maintains a complaint structure which involves the Committee of Enquiry and the Disciplinary Committee. The code addresses several key issues – integrity, confidentiality, impartiality, responsibility, relationship to the CSSA and non-discrimination.

4.2.1 Integrity

This principle required that member must:

- Behave at all times with integrity:
    - Not knowingly lay claim to a level of competence not possessed.
    - At all times exercise competence at least to the level claimed.
- Will act with complete loyalty towards a client when entrusted with confidential information.
- Will act with impartiality when purporting to give independent advice and must disclose any relevant interests.
- Will accept full responsibility for any work undertaken and will construct and deliver that which has been agreed to.
- Will not seek personal advantage to the detriment of the Institute and will actively seek to enhance the image of the Institute.
- Will not engage in discriminatory practices in professional activities on any basis whatsoever.

4.2.2 Confidentiality

A member will act with complete loyalty towards a client when entrusted with confidential information. A member shall take adequate measures to ensure the confidentiality of a client's information. A member should not disclose, or permit to be disclosed, or use to personal advantage, any confidential information relating to the affairs of present or previous employers or customers without their prior permission. The principle covers the need to protect confidential data. Various kinds of information can be considered by a client or employer to be confidential. Even the fact that a project exists may be sensitive. Business plans, trade secrets, personal information are all examples of confidential data. Training is required for all staff on measures to ensure confidentiality, to guard against the possibility of a third party intentionally or inadvertently misusing data and to be vigilant for leaks of confidentiality arising from careless use of data or indiscretions.

4.2.3 Impartiality

A member will act with impartiality when purporting to give independent advice and will disclose any relevant interests." The principle is primarily directed to the case where a member or members' relatives or friends may make a private profit if the client or employer follows advice given. Any such interest should be disclosed in advance. A second interpretation is where there is no immediate personal profit but the future business or scope of influence of the department depends on a certain solution being accepted. Whereas salespersons are assumed to have a bias towards their own company, an internal consultant should always consider the welfare of the organization as a whole and not just the increased application of computers.

4.2.4 Responsibility

Member must take full responsibility for any work done and the work should be completed in agreed time and budget. In cases of delay, the client must be alerted to any late delivery. Additionally, generic information (not confidential information) about an area should be fed back to the Profession. Members are also required to combat ignorance about technology.

4.2.5 Relationship with IITPSA

Member must:

- Not seek personal advantage to the detriment of the society
- Actively seek to enhance the image of the Society
- Not bring the Society into disrepute by personal behaviour
- Not misrepresent the views of the society
- When faced with conflict of interest, declare their position

4.2.6 Non-discrimination

Member must not engage in illegal discriminatory practices on any bases and must hire personnel based on skills, experience and performance. Remuneration must be done on equal opportunity basis. Additionally, employers should initiate and/or support programs that encourage development and training on equal opportunity basis.

4.2.7 Disciplinary Procedure

This procedure exists so that anyone may lay a complaint against a member. The level of the member determines his/her responsibility. For example, consultants carry more obligations. The Society, however, has no legal standing between member and employer, but where appropriate the Society will give support to member losing job or censuring employer for violating the Society's code of conduct.

The society has regulations that required all complaints to be in writing. The complaint will first be investigated by a Committee of Enquiry which has the power to summon the member involved. If misconduct is established by the committee, the member is given 21 days to response to the complaints. If this response is unsatisfactory, the issue is referred to the Disciplinary Committee.

The Disciplinary Committee sets a formal hearing where witnesses may be called. No legal representation is allowed and the proceeding is carried out in camera. If the member is found to be guilty, he or she can be warned, reprimanded, suspended or expelled.

Activity 1

Do you think this procedure is fair, adequate, and constitutional?

4.3 IITPSA Code of Practice

This Code of Practice is directed to all professional members of IITPSA. It consists, essentially, of a series of statements that prescribe minimum standards of practice, to be observed by members. The Code is concerned with professional responsibility. All members have responsibilities – to clients, to users, to the State and to society at large. Those members who are employees also have responsibilities to their employers and employers' customers and, often, to a Trade Union.

- Personal Development
- Organisation and Management
- Contracting
- Privacy, Security and Integrity
- Development of a System
- Implementation
- Live Systems

A summary of the Code of Practice is provided here. The full code is accessible on the IITPSA website.

4.3.1 Personal Requirements

Statement	**Rationale**
Make sure that members and their subordinates are kept up to date on new technologies, practices, legal requirements and standards	Others will expect this of you
Ensure that subordinates are trained and that this is based on equal opportunity basis	Improve subordinates effectiveness and advancement opportunities
Only accept work for which you are competent or else obtain additional expertise first	Be aware of your own limitation and your duty to the client
Seek opportunities for increasing efficiency	As a professional you should be eliminated inefficiencies and be innovative by using new methods.

4.3.2 Organization and Management

Statement	**Rationale**
Plan, establish and review objectives for both yourself and your subordinates	Keep overall objectives of the project in mind and use well established management practices to keep track.
Ensure tasks are allocated to people according to their ability and competence	Need to balance competence of subordinate to the job, their need to learn new things and responsibility to the client
Establish and maintain channels of communication to seniors, equals and subordinates	Effective communication improves quality of the job and this can be improved by formal training
Be accountable for quality, timeliness and use of resources	Professionalism implies provision of agreed level of service, timeliness and within budget

4.3.3 Contracting

Statement	**Rationale**
Seek expert advice in preparation of formal contract	Contract needs to meet the needs of both parties. Member should use specialists where necessary (e.g. Tax and risk evaluation)
Adequately cover all requirements and responsibilities	Professional status implies that all details are covered

4.3.4 Privacy, Security and Integrity

Statement	**Rationale**
Ascertain and evaluate all risks with respect to cost, effectiveness and security level	Essential to determine what value would be lost if security is breached. Allocate to the areas of protection, detection, suppression and recovery.
Recommend appropriate security levels to risks	Risks can be mandatory (e.g. health and safety) or non-mandatory (e.g. security of data etc).
Apply, monitor and report on the effectiveness of the levels of security	People can become lax. Employment of new technology maybe appropriate (e.g. when combating new attacks)

Statement	Rationale
Ensure all staff is trained to protect life, data and equipments in cases of disaster.	Safety of people is the first priority. Backup facilities for programs, data are essential because of consequential losses.
Need to take all reasonable steps to protect confidential information	People's private information is at the root of an individual's right to privacy
Competent people must be in charge of accuracy and integrity of data	Staff assigned to a job must be competent and adequately trained for the job.
An individual must have the right to review their data, correct it and appeal if necessary	Individual has a right to freedom.

4.3.5 Development

Statement	Rationale
Exercise impartiality when evaluating each project	Impartiality is a Professional imperative
Effectively plan, monitor, adjust and report on all aspects of the project	Need to control all aspects of a project
Use standard procedures and ensure that documentation is available and used.	Professionalism implies using standard, accepted, appropriate procedures. People should know how, when, or who must do the work.
Specify system objectives, completion data, cost, security requirements and acceptance requirements.	Clear statement of objective, agreed by client must be the rationale of the project.
Client should participate in all stages of analysis, development and implementation	The system is for the client. The closer the client's involvement the better the system will be
Tasks completed within job in a defined order	Plan the system logically
Specify and conduct program and system tests	Show system functions as intended, as well as detect and eliminate errors.
Ensure design is sufficiently documented to facilitate audit, maintenance, enhancement and comprehension by user	Ensure system is usable
I/O designed for easy use Data that is erroneous, redundant or out of date must be easily changed or deleted, if necessary	Simple I/O ensures less errors and easier acceptance. Data must be correct while the privacy of individual is respected.
Backup procedures for data and programs	Consequential losses need to be minimized
Ensure projects are technically sound, use most appropriate technology, while staying within time/cost constraints	Professional should solve the clients problem in the most appropriate manner

4.3.6 Implementation

Statement	Rationale
Provide adequate provision for staff training	System will not work properly unless staff knows how to use it. Education of users empowers them and allays fears of new system.
Changeover to new operational system – plan it, monitor the transition, adjust if necessary and report	Ensure new operation works well

4.3.7 Live Systems

Statement	Rationale
Plan and operate efficient and reliable processing within the budget	Reliability and efficiency is expected of a professional
Monitor performance and quality. Hold review regularly to assess efficiency, effectiveness and security	Requirements of systems change with time hence the need for review
Plan for maintenance and enhancements	Correct errors and upgrade system
Keep good liaison with users and set up mechanism for dealing with queries	Ensure any problems are dealt with quickly and appropriately.

4.4 BCS Codes of Conduct and Practice

The British Computer Society (BCS) [http://www.bcs.org] sets the professional standards of competence, conduct and ethical practice for computing in the United Kingdom. The Royal Charter incorporated the Society in July 1984. This code of conduct is directed to all members of The British Computer Society. As an aid to understanding, these rules have been grouped into the principal duties, which all members should endeavour to discharge in pursuing their professional lives:

- The Public Interest.
- Professional Competence and Integrity.
- Duty to Relevant Authority.
- Duty to the Profession.

4.4.1 The BCS Code of Conduct

The Public Interest

A member shall:

- have due regard for public health, privacy, security and wellbeing of others and the environment.
- have due regard for the legitimate rights of Third Parties*.
- conduct their professional activities without discrimination on the grounds of sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or disability, or of any other condition or requirement
- promote equal access to the benefits of IT and seek to promote the inclusion of all sectors in society wherever opportunities arise.

Professional Competence and Integrity

A member shall:

- only undertake to do work or provide a service that is within your professional competence.
- NOT claim any level of competence that you do not possess.
- develop their professional knowledge, skills and competence on a continuing basis, maintaining awareness of technological developments, procedures, and standards that are relevant to your field.
- ensure that they have the knowledge and understanding of Legislation* and that you comply with such Legislation, in carrying out your professional responsibilities.
- respect and value alternative viewpoints and, seek, accept and offer honest criticisms of work.
- avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction.
- reject and will not make any offer of bribery or unethical inducement.

Duty to Relevant Authority

A member shall:

- carry out their professional responsibilities with due care and diligence in accordance with the Relevant

Authority’s requirements whilst exercising your professional judgement at all times.

- seek to avoid any situation that may give rise to a conflict of interest between you and your Relevant Authority.
- accept professional responsibility for their work and for the work of colleagues who are defined in a given context as working under your supervision.
- NOT disclose or authorise to be disclosed, or use for personal gain or to benefit a third party, confidential information except with the permission of your Relevant Authority, or as required by Legislation
- NOT misrepresent or withhold information on the performance of products, systems or services (unless lawfully bound by a duty of confidentiality not to disclose such information), or take advantage of the lack of relevant knowledge or inexperience of others.

Duty to the Profession

A member shall:

- accept their personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute.
- seek to improve professional standards through participation in their development, use and enforcement.
- uphold the reputation and good standing of BCS, the Chartered Institute for IT.
- act with integrity and respect in their professional relationships with all members of BCS and with members of other professions with whom you work in a professional capacity.
- notify BCS if convicted of a criminal offence or upon becoming bankrupt or disqualified as a Company Director and in each case give details of the relevant jurisdiction.
- encourage and support fellow members in their professional development.

4.4.2 The BCS Code of Practice

The British Computer Society Code of Practice is directed to all members of The British Computer Society. It consists, essentially, of a series of statements, which prescribe minimum standards of practice, to be observed by all members.

The Code of Practice is concerned with professional responsibility. All members have responsibilities: to clients, to users, to the State and society at large. Those members who are employees also have responsibilities to their employers and employers' customers and, often, to a Trade Union. In the event of apparent clash in responsibilities, obligations or prescribed practice the Society's Secretary-General should be consulted at the earliest opportunity.

The Code is to be viewed as a whole: individual parts are not intended to be used in isolation to justify errors or omissions or commission. The Code is intended to be observed in the spirit and not merely the word. The BCS membership covers all occupations relevant to the use of computers and it is not possible to define the Code in terms directly relevant to each individual member. For this reason the Code is set out in two levels to enable every member to reach appropriate interpretations.

The BCS Code of Practice can be found at the following Web site: http://www.bcs.org/

Activity 2: Comparing Codes

Compare and contrast CSSA's codes to that of BCS. What are the differences and similarities. Also have a look at the ACM Code of Ethics and Professional Conduct [http://www.acm.org/about/code-of-ethics].

Chapter 5. Privacy

Table of Contents

5.1 Scenarios

5.1.1 Scenario 1: Fund Raising and Potential Donors

Jan studies computer science at university but does not major in it. She wishes to be involved in public service and so accepts a fund-raising job for a big university. She is asked to get information on Frank – a potential donor. Frank has been recommended by another donor who said that Frank is keen on providing some funds to the university but has not previously donated to this university.

Jan was asked to find out about all the information on Frank, with special focus on his wealth and the likely area where Frank will be most keen. Using the Internet and databases, Jan was able to find out the following:

- Via a public database, his board memberships
- Via databases of associated organisations, contributions he has made to others and his support for any religious organisations
- Newspaper archives – information written about Frank
- Governmental records – if he has had any encounter with the law
- Credit card agencies – his credit history

Other routes that Jan tried to get information include:

- Contacting Amazon.com about the types of books he read
- Wonders if his ISP will tell her about his online activities
- From the university records she finds that he was treated at the university hospital.
- She finds that she can access his medical records and discovers that he was treated successfully for a kidney complaint

She then proceeds to recommends that he be approached for a donation for kidney research.

Activity 1

Discuss whether or not you think she has done anything wrong?

5.1.2 Scenario 2: Taking work home

Max works for a government department working against alcoholism and drug abuse. The department maintains a database of people with these problems. Max's job is to track the success or failure of treatment programs. He has to prepare a report indicating:

- Number of clients seen per month in each program
- Length of client treatment
- Criminal history of clients
- Distribution addresses

He gets this information from various databases located in different locations. To do this, he downloads information to his computer in his office, then copies the data to a portable hard drive and takes that home to finish his report there. However, he also leaves a copy of the information and the report on his machine at home.

Activity 2

Is he wrong to move the data to his house and is he wrong to leave the data there when he is done with the report. What policy should Max's agency have concerning taking work home? Discuss.

5.1.3 Scenario 3: Workplace Monitoring

Estelle works for Medical Insurance Company. She supervises the claims department and her brief is to improve efficiency there – each unit must process a minimum number of claims per day. In order to achieve this goal, she installs a software system which monitors:

- The number of claims processed by each clerk
- Number of keystrokes done by each clerk
- Log information on when each clerk is on or off his/her post

The system allows her to watch all the above information in real-time on her screen. She can also see all e-mails sent by each clerk regardless of whether the e-mail is business-related or not.

Activity 3

Should she use this system and if so should each of the clerk be informed? Do you think any limitations should be placed on companies employing such systems? Discuss.

5.1.4 Scenario 4: Data Mining

Ravi works for a credit card company, developing new products. He read about data mining and convinces his supervisor to buy this tool. With this tool Ravi can get information on customers' buying habits, as well as finds out postal codes correlation to loan defaults. Based on this new information a new policy can be formulated resulting in his company refusing credits to clients in 'bad' postal code areas. Doing this could reduce his company's exposure to bad loans.

Ravi also discovers that Zoroastrians who donate to charity charges a substantial amount to their credit cards. He promptly recommends a new policy of soliciting more Zoroastrians for credit card in hope of increasing his company's profit.

Activity 4

Are either of these two recommendations wrong? What about the way Ravi use these information? Is the company wrong by implement these policies? Discuss.

5.2 Is there anything new here?

Panopticon of J. Bentham 1787 involves the design of prisons. By arranging the cells in circle (with the guard in the centre) in such a way that the guard can see prisoners but vice versa, the guard needs not even be there all the time. When individuals (in this case, prisoners) believe that they are being watched, they behave differently as they are concern with the observers and what they might think of them.

Many experts think that information gathering is like Panopticon. Information gather itself is not new – governmental and private organisations have always kept databases. The difference is that much more surveillance can be made with electronic databases because of their speed, types of information and scale of exchange of information between them.

Activity 5

Compare and contrast paper-based and electronic records in more detail – pay particular attention on the amount and type of data, who has access to them and the length of retention.

5.2.1 Max's case

Recall that Max takes sensitive data home. The movement of data can be problematic in itself – it is difficult to keep track and to ensure security of the data in different environments and locations. Taking work home is not new – companies have allowed their employee to take company's resources home, make use of it in completed a tasks and then to bring it back. In these cases, companies have strict rules on how these resources should be handled. Computer data should be treated in a similar way – by either not allowing data to be copied from the main frame at all or by specifying data encryption to be used.

5.2.2 Access to data

Consider the case of Pat who took her landlord to court because of presence of pests in the flat. The landlord did not contest the case, but soon after Pat moved to another area but discovered that she always get turned down. Pat discovers that there is a list of people who has taken landlords to court and that this list can be purchased.

Activity 6

Do you think anyone is at fault here? Can you see the parallel between this lo-tech database and the use of much more sophisticated databases for similar reasons, as in Ravi's case?

5.3 Understanding the 'Computer and Privacy' Issue

In essence the issue revolves around:

- Collection and use of data.
- Information obtained from data versus loss of privacy.
- The needs of the organisation collecting and using the information versus individuals' right of privacy (considered a social good).

An example is that Amazon collects information on its clients in order to be able to inform them of new books in their interest areas.

5.3.1 Personal Privacy

What is personal privacy and why is it valuable? Most people expect privacy in their personal space such as home – the domain in which government and other organisations should not interfere. Privacy is often seen as intrinsic good – good in itself – which can lead to other good. Kant's theory is that privacy is essential to autonomy and that autonomy is inconceivable without privacy.

Technological development has not only changed how business is conducted, but also has had a huge impact on personal and community identities.

Activity 7

Read the following paragraph:

> *In order to establish a relationship with an individual one needs to be able to control information about oneself in order to maintain a relationship. Collecting and grouping of information into a database causes us to lose control of the information. This loss of control reduces our ability to form relationships.*

Do you agree with what is being said there? Do not consider just personal relationships consider professional relationships as well. When you are chatting or emailing on the Net, nobody knows who you are by anything other than the name you have given as your identity. Your physical characteristics — skin colour, height, physical features — are unknown. Your on-line characteristics are formed by your messages. What is known about you is only the image that you choose to give of yourself.

Impact on the Individual

Identity: Anonymity can be liberating. Other users you come in contact with on the Net cannot look at your physical self or hear your accent and make assumptions about you. You are judged on the opinions and information you express.

Intrusion on Privacy: Personal information can be captured at certain sites through the information you have provided when you make an on-line transaction, or by tracking the user by using cookies. Data may be captured and analyzed without either the user's knowledge or consent. Their surfing patterns are collected and analyzed to classify them into marketing categories. Many companies now monitor employee e-mail, their argument being that any email leaving the company is the business of the company. Should anyone wish to contact an employee with urgent personal information there is a risk that this could become public knowledge.

5.3.2 Individual – Organizational Relationships

It is said that information a person gives to an organisation empowers them over the person – for example, a credit card company. Organisations can establish this relationship without any action by the individual (e.g. Subscription information). This problem has been amplified by the introduction of computers. Government has tried to deal with this and to allay fears by passing laws that prevent different database from being joined (e.g. the Home Affairs' and Police's fingerprints databases). Laws have been passed on the privacy issues concerning medical and credit records amongst others.

In the mid1970s, the United States provided five principles to govern fair information gathering practices:

1. No secret personal data keeping.
2. Individual must be able to discover their personal information and how it is used.
3. Individual must be able to discover and stop information collected for one purpose but is used for another.
4. Individual must be able to correct wrong information.
5. Database administrator of personal information must take necessary precautions to prevent misuse and also to assure reliability of data.

Activity 8

Do you think that these principles are still appropriate today when it comes to electronic databases? What changes, if any, do you think needs to be made to this code? This issue of individual – organisation relationships is discussed further in the section on Privacy Issues on the workplace later in this chapter.

Activity 9

The objective of this exercise is to experiment with some ideas on privacy. Write down some ideas about the following:

- How would you like to portray yourself to others?
- Can this be achieved if contact is only by e-mail?
- What aspect of yourself might others regard as 'detrimental'?
- Can this be hidden if contact is only by e-mail?
- What feature of email allows this type of privacy?

You can find some thoughts about this activity at the end of the unit.

5.3.3 Global Perspective

Legislators, theologians, scientists, academics and business people are getting more interested in the impact of information technology on individuals, organizations and communities. The possible outcomes in the near future could be better — not necessarily stricter — legislation safeguarding user privacy, increased education in the proper use of the Internet, and more options for technological control that can be implemented based on user discretion. The alternative outcomes could be strict tracking of every user, together with numerous legislative bodies all imposing their own views on what information should be available. The challenge ahead of us is to ensure that the benefits of the Internet far outweigh the real and serious threats brought about by the information revolution.

The Internet expansion plays a large role in increasing the potential for misusing of information. The information is flowing across borders more readily and frequently. Irrespective of the individual nation's policies, there is still a need for a global policy. European Union has a policy that is enforced amongst its members. Each member states must make sure that personal data must be:

- Processed fairly and lawfully.
- Collected for specific and legitimate purposes.
- Not processed further (except for statistical, scientific or historical reasons and then with prior permission).
- Adequate but not excessive for purpose required.
- Kept up to date.
- Accurate for purpose collected.
- Kept no longer than required.

Activity 10

Read the articles supplied online as part of this unit (Guardian newspaper articles).

- Do you think that a service that is free to users should be more secure? After all, you only get what you pay for.
- Will this event change the way you use e-mail?
- Do you think that independent bodies should check statements claiming privacy for these types of services?

You can find some thoughts about this activity at the end of the unit.

5.3.4 Proposal for better Protection

There have also been many proposals for better protection with broad conceptual changes and legislative initiatives:

- Appreciate and action the principle that privacy is a social good.
- Need for a comprehensive approach that is not a piecemeal approach but also integrate a global exchange of data?
- Power of private corporations never envisaged – this is a new vacuum.
- Sweden introduces the Data Inspection Board:
  - Licences all automated personal information systems in both public and private sectors.
  - Controls collection of personal data.
  - Can investigate completes.
  - Designs rules for personal data collection.

Activity 11

Discuss the pro and con of a system such as that of Sweden's Data Inspection Board is. Do you think that each country should go this route?

The ACM's code of conduct considers privacy and seeks to:

- Minimise data collected.

- Only allow authorised access to data.
- Provide proper security.
- Determine required retention period.
- Ensure proper disposal of the data.

5.4 Effects of IT on recording keeping

Information keeping and handling is not new but information technology has changed record keeping in the following ways:

- Scale of information keeping
- New kinds of information kept
- New scale of information distribution and exchange
- Effect of erroneous data magnified
- Information can endure for much longer

5.5 Privacy Issues in the workplace

Recall scenario 2 with Estelle and her monitoring software. Were your generally for, against or undecided against computer monitoring in the workplace. Your feeling is likely to be different depending on whether you are an employer or an employee – but here are some arguments for and against:

5.5.1 Arguments for Computer Monitoring in the Workplace

That it is also used to provide incentives for employees and effectively rewards individuals for true merit and reward. They also point out that what is being measured is factual and hard, and that workers tend to favour such systems, they have seen too many cases of the wrong people being promoted for the wrong reasons. With the facts that the computer gathers, diligent workers can legitimately argue a case for better pay and conditions and this case does not rely upon personal opinions and personalities. Furthermore, these systems can help eliminate rampant waste, for example, employees calling long distance for private uses, a team carrying the load for an unproductive team member, identifying the theft of materials by matching the stock used with the amount processed by line workers (and discovering discrepancies). Finally, monitoring on a computer network can assist in troubleshooting and fine tuning of a system, as well as streamlining job design and fairly apportioning workloads.

5.5.2 Arguments against Computer Monitoring in the Workplace

However, there is also the danger of turning workers into better paid battery hens, denying them job satisfaction and eliminating the human element from their work. For example, although reservation clerks may be given an incentive to process more calls when they are being monitored, it may also eliminate any human spontaneity or friendliness in their communication. There is question of balance between the rights and expectations of employees versus the obligations and objectives of employers.

Forestor and Morrison (1990) state that clearly profits are important to the continued functioning of capitalist societies and profit itself is dependent upon competitiveness. However, just how far we are willing to proceed in the pursuit of competitiveness and profitability is a matter of judgement. For example, the use of cheap child labour was once regarded as a sensible business strategy, but now our ethical sense and labour protection laws prohibit this practice. It remains to be seen in which direction our ethical intuitions will take us in determining the nature of future employment, whether we can all be monitored in the interest of profit and accountability, or whether we shall see a renewed interest in designing jobs for people.

In addition, we need to ask what kind of precedent computer based monitoring of employees will set for other invasive practices. For example, similar arguments can be marshaled for the compulsory drug testing of key personnel such as pilots, train drivers, and power plant operators. If these people have the potential to kill thousands by accident, then do we not have the right to ensure that they are in a fit state to work? On the other hand, why not also monitor the alcohol purchases of convicted drunk drivers? This highlights the most contentious aspect of any form of computer based monitoring: it is not so much the harm it may currently be causing, but what it represents.

Activity 12

Has your view changed after reading the arguments above? What is your view now? Discuss this issue with other students if you can.

5.6 Interception Act versus Privacy Act (South Africa)

Two important acts concerning privacy were introduced to the South African public. The interception act was amended in 2010.

5.6.1 The Interception Act

The interception act came into full effect in September 2005 (http://www.justice.gov.za/legislation/acts/2002-070.pdf). (Full title: the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA)). RICA seeks to regulate the interaction of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information. In order to be able to monitor communication the following steps must be taken:

- Law enforcement must be in possession of information or evident that electronic communications are being used in the commission of the crime.

- They must approach the court and request an "interception direction". The sitting judge will then decide on the merit of the evident present and will grant or refuse this directive.

- Once the interception direction is obtained, it can then be served to the relevant service provider who is then required by law to monitor any communication made by the individual or party concerned and then to forward all surveillance information to the law enforcement agency. Note that the person under surveillance needs not be informed.

RICA provides that all forms of monitoring and interception of communications are unlawful unless the monitoring and interception takes place under one of the recognized exceptions in RICA. There are several exceptions to the general rule on the prohibition on intercepting communications, three of which apply to monitoring in the workplace:

- **Party to a communication:** Section 4 of the RICA allows a party to a communication to monitor and intercept the communication if he/she is a party to the communication (for example, where the participants in a meeting consent to the meeting being recorded). This exception also applies where the interceptor is acting with the consent of one of the parties to the communication.
- **Written Consent:** Section 5 allows for interception of any communication under any circumstances – i.e. no special motivation or reason is required for it provided the person whose communication is being intercepted has consented to it in writing prior to such interception.
- **Business Purpose Exception:** Section 6 contains a so-called “business purpose exception” which involves the interception of “indirect communications in connection with the carrying on of business”. Section 6 authorises any person to intercept indirect communications in the course of carrying out their

business by means of which a transaction is concluded in the course of that business, which “otherwise relates to that business” or which “otherwise takes place in the course of the carrying on of that business, in the course of its transmission over a telecommunication system”.

5.6.2 The Privacy Act

The protection of personal information Act [http://www.gov.za/sites/www.gov.za/files/37067_26-11_Act4of2013ProtectionOfPersonalInfor_correct.pdf] is seen by some as a counterbalance to the Interception Act above. The act seeks to promote the protection of personal information of South Africans processed by public and private bodies. It also seeks to provide for the rights of persons regarding unsolicited electronic communications and automated decision making. It also seeks to regulate the flow of personal information across the borders of the Republic.

Activity 11

It is likely that by the time you are reading this set of notes that another draft of the proposed act has been released. The media might also be covering it in more detail. Try and get hold of the most recent draft or some analysis of it in the media. How has it changed?

Activity 12

Discuss if and how the interception and privacy counterbalance one another. Do you have concerns about either of the acts?

5.7 Protect Your Online Privacy

The Electronic Frontier Foundation (EFF) [http://www.eff.org] is an organisation that protects rights and promotes freedom in the electronic frontier, including an individuals basic right to privacy. They advocate the following twelve ways to protect your online privacy.

5.7.1 Do not reveal personal information inadvertently

You may be "shedding" personal details, including e-mail addresses and other contact information, without even knowing it unless you properly configure your Web browser. In your browser's "Setup", "Options" or "Preferences" menus, you may wish to use a pseudonym instead of your real name, and not enter an e-mail address, nor provide other personally identifiable information that you don't wish to share. When visiting a site you trust you can choose to give them your info, in forms on their site; there is no need for your browser to potentially make this information available to all comers. Also be on the lookout for system wide "Internet defaults" programs on your computer (some examples include Window's Internet Control Panel, and MacOS's Configuration Manager, and the third party Mac utility named Internet Config). While they are useful for various things, like keeping multiple Web browser and other Internet tools consistent in how the treat downloaded files and such, they should probably also be anonymised just like your browser itself, if they contain any fields for personal information. Households with children may have an additional security problem - have you set clear rules for your children, so that they know not to reveal personal information unless you OK it on a site-by-site basis?

5.7.2 Turn on cookie notices in your Web browser, and/or use cookie management software

Cookies are a small amount of information that Web sites store on your computer, temporarily or more-or-less permanently. In many cases cookies are useful and innocuous. They may be passwords and user IDs, so that you do not have to keep retyping them every time you load a new page at the site that issued the cookie. Other cookies however, can be used for "data mining" purposes, to track your motions through a Web site, the time you spend there, what links you click on and other details that the company wants to record, usually for marketing purposes. Most cookies can only be read by the party that created them. However, some companies that manage online banner advertising are, in essence, cookie sharing rings. They can track which pages you load, which ads you click on, etc., and share this information with all of their client Web sites (who may number in the hundreds, even thousands.) It is unknown whether all of these cookie rings (some examples of which are Double Click and Link Exchange) do in fact share user data, but they certainly can do so potentially.

Browsers are starting to allow user control over cookies. Mozilla and Firefox, for example, allows you to see a notice when a site tries to write a cookie file to your hard drive, and gives you some information about it, allowing you to decide whether or not to accept it. (Be on the lookout for cookies the function of which is not apparent, which go to other sites than the one you are trying to load, or which are not temporary). It also allows you to automatically block all cookies that are being sent to third parties (or to block all cookies, entirely, but this will make some sites inoperable). Internet Explorer has a cookie management interface in addition to Netscape like features, allowing you to selectively enable or disable cookies on a site by site basis, even to allow cookies for a site generally, but delete a specific cookie you are suspicious about. With Internet Explorer you can also turn on cookies for a site temporarily then disable them when you no longer need them. For example, at an online bookstore that requires cookies to process an order, but whom you don't want to track what books you are looking at, what links you are following, etc., the rest of the time. Turning on cookie warnings will cause alert boxes to pop up, but after some practice you may learn to hit "Decline" so fast that you hardly notice them anymore. The idea is to only enable cookies on sites that require them AND whom you trust.

5.7.3 Keep a "clean" e-mail address

When mailing to unknown parties; posting to newsgroups, mailing lists, chat rooms and other public spaces on the Net; or publishing a Web page that mentions your e-mail address, it is best to do this from a "side" account some pseudonymous or simply alternate address, and to use your main or preferred address only on small, members only lists and with known, trusted individuals. Addresses that are posted (even as part of message headers) in public spaces can be easily discovered by spammers (online junk mailers) and added to their list of targets. If your public "throw away" address gets spammed enough to become annoying, you can simply kill it off, and start a new one. Your friends, boss, etc., will still know your "real" address. You can use a free (advertising supported) e-mail service provider like Google or Hotmail for such "side" accounts. It is best to use a "real" Internet service provider for your main account, and to examine their privacy policies and terms of service, as some "free mail" services may have poor privacy track records. You may find it works best to use an e-mail package that allows multiple user IDs and addresses (i.e. "personalities", "aliases") so that you do not have to switch between multiple programs to manage and use more than one e-mail address.

5.7.4 Don't reveal personal details to strangers or just met "friends"

The speed of the Internet is often reflected in rapid online acquaintanceships and friendships. But it is important to realise that you don't really know who these people are or what they are like in real life. A thousand miles away, you don't have friends of friends or other references about this person. Be also wary of face-to-face meetings. If you and your new e-friend wish to meet in person, do it in a public place. Bringing a friend along can also be a good idea. One needn't be paranoid, but one should not be an easy mark, either. Some personal information you might wish to withhold until you know someone much better would include your full name, place of employment, phone number, and street address (among more obvious things like credit card numbers, etc.) Needless to say, such information should not be put on personal home pages. (If you have a work home page, it may well have work contact information on it, but you needn't reveal this page to everyone you meet in a chat room.) For this an (sic) other reasons, many people maintain two personal home pages, a work related one, and an "off duty" version.

Realise you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer. In most countries (including South Africa), employees have little if any privacy protection from monitoring by employers. When discussing sensitive matters in e-mail or other online media, be certain who you are talking you. If you replied to a mailing list post, check the headers - is your reply going to the person you think it is, or to the whole list? Also be aware that an increasing number of employers are monitoring and recording employee Web usage, as well as email. This could compromise home banking passwords and other sensitive information. Keep private data and private Net usage private, at home.

5.7.5 Beware sites that offer some sort of reward or

prize in exchange for your contact or other information

There's a high probability that they are gathering this information for direct marketing purposes. In many cases your name and address are worth much more to them (because they can sell it to other marketers, who can do the same again - a snowball effect) than what you are (supposedly) getting from them. Be especially wary of sweepstakes and contests. You probably won't win, but the marketer sure will if you give them your information.

5.7.6 Do not reply to spammers, for any reason

Spam, or unsolicited bulk e-mail, is something you are probably already familiar with (and tired of). If you get a spammed advertisement, certainly don't take the sender up on whatever offer they are making, but also don't bother replying with "REMOVE" in the subject line, or whatever (probably bogus) unsubscribe instructions you've been given). This simply confirms that your address is being read by a real person, and you'll find yourself on dozens more spammer's lists in no time. If you open the message, watch your outgoing mail queue to make sure that a "return receipt" message was not generated, to be sent back to the spammer automatically. (It is best to queue your mail and send manually, rather than send immediately, so that you can see what's about to go out before it's actually sent.) If you have a good Internet service provider, you may be able to forward copies of spam e-mail to the system administrators. They can route a complaint to the ISP of the spammer (or if you know a lot about mail headers and DNS tools, you can probably contact these ISPs yourself to complain about the spammer.)

5.7.7 Be conscious of Web security

Never submit a credit card number or other highly sensitive personal information without first making sure your connection is secure (encrypted). In Firefox, look for an closed lock (Windows) or unbroken key (Mac) icon at the bottom of the browser window. In Internet Explorer, look for a closed lock icon at the bottom (Windows) or near the top (Mac) of the browser window. In any browser, look at the URL (Web address) line - a secure connection will begin "https://" instead of "http://". If you are at page (sic) that asks for such information but shows "http://" try adding the "s" yourself and hitting enter to reload the page (for Netscape or Internet Explorer; use whatever method is required by your browser to reload the page at the new URL). If you get an error message that the page or site does not exist, this probably means that the company is so clue less - and careless with your information and your money - that they don't even have Web security. Take your business elsewhere.

5.7.8 Be conscious of home computer security

On the other side of the coin, your own computer may be a trouble spot for Internet security. If you have an ADSL line or other connection to the Internet that is up and running 24 hours, unlike a modem and phone line connection, be sure to turn your computer off when you are not using it. Most home PCs have pitifully poor security compared to the Unix workstations that power most commercial Web sites. System crackers search for vulnerable, unattended ADSL connected home computers, and can invade them with surprising ease, searching through files looking for credit card numbers or other sensitive data. They can even take over the computer and quietly using it for their own purposes, such as launching attacks on other computers elsewhere - attacks you could initially be blamed for.

5.7.9 Examine privacy policies and seals

When you are considering whether or not to do business with a Web site, there are other factors than a secure connection you have to consider that are equally important to Web security. Does the site provide off-line contact information, including a postal address? Does the site have a prominently posted privacy policy? If so, what does it say? (Just because they call it a "privacy policy" doesn't mean it will protect you - read it for yourself. Many are little more than disclaimers saying that you have no privacy! So read them carefully.) If the policy sounds OK to you, do you have a reason to believe it? Have you ever heard of this company? What is their reputation? And are they backing up their privacy statement with a seal program such as TRUSTe [http://www.truste.org] or BBBonline [http:// www.bbbonline.org]? (Such programs hold Web sites to some baseline standards, and may revoke seal licenses, with much fanfare, of bad acting companies that do not keep their word.) If you see a seal, is it real? Check with the seal-issuing site to make sure that the seal isn't a fake. And examine terms carefully, especially if you are subscribing to a service rather than buying a product. Look out for auto rebilling scams and hidden fees.

5.7.10 Remember that YOU decide what information about yourself to reveal, when, why, and to whom

Don't give out personally identifiable information too easily. Just as you might think twice about giving some clerk at the mall your home address and phone number, keep in mind that simply because a site asks for or demands personal information from you does not mean you have to give it. You do have to give accurate billing information if you are buying something, of course, but if you are registering with a free site that is a little too nosy for you, there is no law against providing them with pseudonymous information. (However, it would probably be polite to use obviously fake addresses, such as "123 No Such Street, Nowhere, NW 0010, Republic of Nowhereland". If they are generating mailings based on this information presumably in accordance with the terms of their privacy policy - they can probably weed such addresses out and not waste the postage on them.)

5.7.11 Use encryption

Last but certainly not least, there are other privacy threats besides abusive marketers, nosy bosses, spammers and scammers. Some of the threats include industrial espionage, government surveillance, identity theft, disgruntled former associates, and system crackers. Relatively easy to use e-mail and file encryption software is available for free, such as Pretty Good Privacy (PGP) [http://www.pgpi.org], which runs on almost all computers and even integrates seamlessly with most major e-mail software. Good encryption uses very robust secret codes, which are difficult if not impossible to crack, to protect your data. You can also use specialised services (some free, some pay), such as the Anonymizer [http:// www.anonymizer.com], which can completely disguise to Web sites where you are coming from and who you are (and block all cookies). Some ISPs are beginning to offer secure, encrypted dial up accounts and other security features. Hopefully some day soon, good encryption and computer security will simply be included in all such services, but for now you have to actively seek out good service.

5.8 More on Encryption

In an open network such as the Internet, message privacy, particularly for e-commerce transactions, requires encryption and decryption.

5.8.1 PGP (Pretty Good Privacy)

PGP is a popular program used to encrypt and decrypt e-mail over the Internet. It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity and know that the message was not changed en route. Available both as freeware and in a low-cost commercial version, PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations. Developed by Philip R. Zimmermann in 1991, PGP has become a de facto standard for e-mail security. PGP can also be used to encrypt files being stored so that they are unreadable by other users or intruders.

5.8.2 How It Works

PGP uses a variation of the public key system. In a public key system, each user has a publicly known encryption key and a private key known only to that user. You encrypt a message you send to someone else using their public key. When they receive it, they decrypt it using their private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message. (In other words this is a two stage-encryption process.)

PGP comes in two public key versions - RSA and Diffie-Hellman. The RSA version, for which PGP must pay a license fee to RSA, uses the IDEA algorithm to generate a short key for the entire message and RSA to encrypt the short key. The Diffie-Hellman version uses the CAST algorithm for the short key to encrypt the message and the Diffie-Hellman algorithm to encrypt the short key.

For sending digital signatures, PGP uses an efficient algorithm that generates a hash code from the user's name and other signature information. This hash code is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, then the receiver is sure that the message has arrived securely from the stated sender. PGP's RSA version uses the MD5 algorithm to generate the hash code. PGP's Diffie-Hellman version uses the SHA-1 algorithm to generate the hash code.

To use PGP, you download or purchase it and install it on your computer system. Typically, it contains a user interface that works with your customary e-mail program. You also need to register the public key that your PGP program gives you with a PGP public key server so that people you exchange messages with will be able to find your public key. Network Associates maintains an LDAP / HTTP public key server that has 300,000 registered public keys. This server is mirrored at other sites around the world.

5.8.3 Where Can You Use PGP

Originally, the U.S. government restricted the exportation of PGP technology. Today, however, PGP encrypted e-mail can be exchanged with users outside the U.S if you have the correct versions of PGP at both ends. Unlike most other encryption products, the international version is just as secure as the domestic version.

The freely available PGP cannot legally be used for commercial purposes - for that, one must obtain the commercial version from Network Associates (formerly PGP, Inc.). There are several versions of PGP in use. Add-ons can be purchased that allow backward compatibility for newer RSA versions with older versions. However, the Diffie-Hellman and RSA versions of PGP do not work with each other since they use different algorithms. This term was originally written by Sabrina Dei Giudici from Web Marketing, Perth, Western Australia.

5.9 Review Questions

1. How can we ensure privacy when using e-mail?
2. What does PICS stand for?
3. Briefly outline two ways in which censorship ratings can be made.
4. Discuss briefly something we could do, if we found an unsuitable website with misleading ratings.
5. Why would a company censor Internet use?
6. What is blocking software?

You can find answers to these review questions at the end of the unit.

5.10 Discussion and Answers

5.10.1 Discussion on Activity 9

1. Tall, dark, handsome, blonde, pretty, honest, cheerful, short, fun, intelligent, average, nice eyes ? (the list goes on ....!)
2. You can be all of these: nobody can tell unless you are using a Web cam (as part of video conferencing), or you tell them.
3. Glasses, big feet, spots, green hair!
4. You cannot tell if the sender of an e-mail message is wearing glasses!

The time to think about your response. In contrast, this is something that is not always possible when we are talking to a friend. It also can be difficult in a chat room to take time.

5.10.2 Discussion on Activity 10

1. There are no clear answers. Those who are aware of e-mail systems know that no e-mail can be totally secure. It is possible for somebody who has access to an Internet server to intercept and pass on e-mail. When the system is Web based the risks are greater, as the mail sits on a Web server until it is collected.

   Security could be terrible but still acceptable if the users were aware of the risks and made sure that any sensitive messages were encrypted.

2. This is your decision. A decision to be cautious is probably a good one.

3. In many countries there are standards set for advertising. This could be extremely useful for consumers as well as advertisers, who would possibly gain credibility if they had registered their advertisement. In the case study, the claim regarding 'privacy' could be removed.

5.10.3 Solutions to Review Questions

These may not be the ultimate answers to the review questions. You should also check with other resources including your textbooks and the Internet.

1. By using a strong encryption method.

2. Platform for Internet Content Selection.

3. The website can be rated by an independent ratings organisation or the author of the site.

4. We could inform our Internet Service provider and inform some of the search engines...Etc.

Chapter 6. Censorship

Table of Contents

6.1 Introduction to Censorship

6.1.1 An Overview

Accessing the Internet is easy. All it requires is a computer, a telecommunications connection, a modem and a browser.

However, providing access to the Internet at work might mean that employees misuse the Internet during office hours. For instance, an employee might make purchases from various Web sites. Providing Internet access at home might mean that children are exposed to information that parents might consider harmful. However, not providing access to the Internet might exclude people from the benefits of the vast information on the Internet. It might be better, then, to filter the websites to ensure the 'right' information is accessible to people such as children and employees. It is also possible for communities to filter out information that they consider 'inappropriate'.

Freedom of Speech is a fundamental human right in many countries. In the United States it is the first and most important amendment to the Constitution. Other countries have legislated Freedom of Speech and Information in other ways. The other side of the censorship coin is the freedom of information, and it is important that we do not suppress this right in our zeal to, for instance, prevent children from viewing pornography.

Activity 1: What could we censor?

The object of this activity is to consider what material different authorities would censor. Make a table with four columns as shown. We have started the table for you to show the kinds of responses required.

The main types of authority are:

- **Parental** — authority over their children.
- **Employer** — authority over their employees in the workplace.
- **Government** — authority over a country.
- **International** — authority over the international community.

Parental	Employer	Government	International
Pornographic material	Games	Violent Materials	Terrorist Newsgroups

Fill in as many types of Web content that you can think of that the authority concerned could be interested in censoring. You may duplicate material types in different columns.

6.1.2 Why Censor?

The following are some of the reasons supporting censorship given by various experts and opinion groups. Feel free to disagree with these, or even to add new ones. Censorship is a contentious issue and a wide range of viewpoints exist on the topic.

- **Parents**: While parents would like their children to benefit from educational Web sites, children can also be easily influenced by the content they find on the Web. In particular, parents want to prevent their children from accessing adult material.
- **Employers**: Employees given Web access may surf the Net during office hours. The cost of the connection is paid for by the employer, and unwanted surfing could lower productivity. Corporate liability may be threatened if employees view inappropriate and/or offensive material.
- **Pressure groups**: An increasing number of independent groups want to deter the publication of offensive material on the Web. They search the Web for sites which they find offensive, such as pornography sites, sites for weapon sales, and hate campaigns. They then campaign for the removal of such sites.
- **Legal**: Many countries have laws that limit the material that may be communicated by electronic means. It is important to consider the laws not only of your own country, but also those that apply in country of the target audience.

6.2 Censorship Strategies

6.2.1 Overview

We investigated the use of metadata in an earlier unit. It is often this data that is used to automatically determine whether a site should be blocked or not. It is also possible for sites to be added to lists of unacceptable or acceptable sites. Some of the popular systems for censoring sites are discussed below.

6.2.2 Blocking Software

Blocking software contains a list of "objectionable" sites which it does not allow the Web browser to access. This list can be updated at the user's discretion. For example, parents may want to allow certain sites to be accessed by their children as they grow older and mature. Surfwatch and Netnanny are examples of such software.

A new alternative is being developed: instead of restricting access to "bad" sites, the software keeps a list of "good" sites to which access is allowed. However, this might be very restrictive as keeping an exhaustive list of "good" sites is difficult, and so many appropriate sites may be blocked.

Activity 2: Investigating Blocking Software

Use your favourite Internet search engines to look for blocking software. NetNanny [http:// www.netnanny.com] might be a good place to start. Focus on what the software claims to do. Note your opinion of each feature and whether you think it is a good idea. Can you offer a better way to achieve this protection?

6.2.3 Ratings

Website content can be classified according to certain labels, similar to those used by the Film and Video Classifications. The Platform for Internet Content Selection (PICS) is a well-known classification rating system that has been developed by the World Wide Web Consortium [http:// www.w3.org/PICS/].

Activity 3: Who is the Censor?

The objective of this exercise is to consider who might be responsible for rating a website. Jot down on a piece of paper two or more groups that could possibly rate a website (e.g. a university website). The Recreational Software Advisory Council (RSAC) is an Internet rating service (http:// www.rsac.org/index.asp). Web developers can register with the service and, by answering some simple questions about their site, receive a PICS based rating of their site. Users can then set their browsers to block access to sites using the RSAC rating categories. This makes site selection more flexible.

Three things must be present for a rating based approach.

1. **Syntax for defining labels:** This is the different aspects of the site to be measured. For example, a website could have labels describing the levels of Language, Nudity, Sex, and Violence.

2. **Syntax for labeling content:** This is a rating classification itself for each of the labels. The each label's criteria have to be determined before giving its value.

3. **Method of retrieving labels.** The labels, for example, could be embedded within the HTML file or kept as a separate file included into the HTML files when they are accessed.

6.2.4 Service Providers

Internet service providers can also enable censorship. They can, for instance, supply different user names and passwords to each family member, or to different management levels in a corporation. Each user is then given a corresponding level of "access authority".

The ISP can then run the appropriate software to block access to sites based on the user's access level. This can be based on block lists or site ratings.

6.2.5 Browsers and search engines

Some browsers and search engines directly allow for censorship. These may use a password system to allow for different levels of access. Some search engines allow for user feedback to provide information used to decide if a site should be removed from their index.

6.2.6 Social Methods

With so much of the emphasis of censorship placed on the individual — whether an employer, parent or website designers — to implement a censorship strategy, it is important that users are educated as to the implications of their actions. There is a moral responsibility associated with data access, and those who have the ability to control it need to be aware of the issues involved. Education plays an important role in raising awareness, and this has to be addressed from a global perspective.

6.3 Censorship and Controversy

Who has the power to decide which sites are "good" or "bad"? Who is in control — the one who rates or the one using the ratings?

6.3.1 Ratings

Ratings usage can be grouped into the following categories

- **Closed group**: The ratings given depend on the criteria set up by the raters. A religious organization would tend to be stricter than a secular educational institute. Therefore the accepted ratings would depend on which rating organization was utilized to perform the rating.
- **Community**: Net Shepherd (a ratings organization) claim that their rating community is a virtual, online community of people who represent the Internet's general population. However, these people may not be representative of the world's population. Studies have shown that Internet users are more affluent and educated than non-users. Thus, the community is self-selecting.

There are many groups of user to which ratings may be applicable:

- **Individual users**: There is no single, familiar labeling system, as with movie film ratings. This can make it complicated to learn the various labels attached to different websites. Again, this brings up the issue of which group to trust.
- **Imposed**: The individual might not be given the option to choose. Restrictions can be placed by a company or by a government that regulates the Web servers in its country. National 'firewalls' are implemented in China and Singapore, blocking certain types of material. Firewalls also exist to 'protect' the computer networks of many institutions around the world — such as universities and local government organizations.

Ratings may not be representative of the majority of the world's population.

Activity 4: A short proposal

The object of this exercise is to consider the issue of personal responsibility involved in making censorship decisions. Write down two lists:

1. Reasons why you think you might be qualified to decide what the inhabitants of your home town could view on the Internet.
2. Reasons why you might not be able to make fair decisions (with regards to 1).

You can find some thoughts about this activity at the end of the unit.

6.3.2 Freedom

A 1960s folk song (Colours. D. Leitch. 1967. Pye) has the lyrics "freedom is a word I rarely use without thinking". This is possibly a very useful philosophy and certainly worth remembering. Freedom may have a completely different meaning to different people. Freedom for a child to cross a busy road on his/her own may place that child in danger. A parent will educate the child as to the nature of such dangers until the child can take responsibility.

As the founder of the World Wide Web, Tim Berners Lee has said that the main idea of the World Wide Web was to allow any and every kind of information to be published and accessed. There are many people advocating the freedom of the Internet. The Electronic Frontier Foundation (http:// www.eff.org/) was set up to 'work in the public interest to protect fundamental civil liberties, including privacy and freedom of expression, in the arena of computers and the Internet'.

6.3.3 Pressure to Control

The pressure to clamp down on the freedom of the Net comes from concern that not all material published is educational or beneficial. Websites with "inappropriate" content might adversely influence children, and possibly many adults. Employees surf sites that have no connection to their tasks as employees, reducing office productivity.

6.4 Investigating Data Trails

6.4.1 Overview

This section investigates how computer systems have intruded into consumers' lives. Often without consumer knowledge or consent, data is collected and distributed to analyze their life patterns. A typical use of the data is to enhance the promotion of business products.

There are three types of trail that will be investigated, although these are not necessarily related to each other. This section will not investigate the ethics of data trails, although it will consider each type's purpose.

6.4.2 Data Trails on Your Machine

Your computer contains information regarding your computer activity. This information is stored whenever you access the Internet. Some of this information is subtle and some of this information is very obvious.

Activity 5: Data Trails on Your Machine

This activity's objective is to investigate some of the data trails that can be found on your computer.

If you are using Microsoft Windows XP, you can view the list of documents that have recently been accessed. This list is available from the *Start* menu and then *My Recent Documents*. The *Start* menu might also show the list of recent applications that you have used.

Your Internet browser will also store history, bookmarks/favourites, cookies (see next section) and other files that you accessed to speed up loading times. Try to learn aboutthese issues with your browsers. Most store this information by default.

What are your conclusions about the availability of information on your machine concerning your Web activity?

You can find some thoughts about this activity at the end of the unit.

It is possible for an employer to analyze the data trails on your machine and also those logged by a Firewall.

6.4.3 Cookies

Sometimes referred to as magic cookies, these are small text or data files (4Kb) left on your machine by a website. They are retrievable at a later date by the website that set them. They can be used for a number of purposes, such as storing browser settings and preferences, thus allowing more efficient downloading of files. They may also store information about websites that you have visited; this allows advertising banners to be effectively targeted. For example, if you were to spend a large amount of time searching the Web for car related topics, the cookie files on your system will inform the organization that set them of your interest in cars, should you return to their server. You would then notice that advertising banners would become car related.

There are lots of software tools that may be used to destroy data trails, however there is always a tradeoff between data trails that are useful and those that can be used to "spy" on your browsing habits.

Activity 6: Data Trails on Other Machines

This Activity's objective is to consider how it may be more difficult than is often assumed to discover what an individual has been browsing from home.

It is reasonably simple for an employer to keep track of data requested by employees. It is more difficult for an Internet service provider (ISP) to track clients.

For this activity consider the ways in which we might be identified as a source for Web page requests. How might this differ when we compare the use of a company network and a home computer connected to an ISP?

Hint: think about what changes each time we log in from home. Write down your ideas.

You can find some thoughts about this activity at the end of the unit.

Surveys inform us that there are many companies tracking their employees' HTML requests and e- mail messages. This is often part of company policy.

6.5 Discussion Topic

The purpose of this exercise is to give you the opportunity to discuss the subject of privacy and censorship.

Before you go to the Discussion Forum you should read over your notes on activity 1 and think about how you would rate your own website, if you have one.

You should then join the Discussion Forum to:

- Discuss your thoughts on whether it is safe to allow people to rate their own websites.
- Share your notes on activity 1. Is there general agreement?
- Discuss whether you think rating should be a compulsory activity either now or in the future when this type of technology becomes less error prone.

6.6 Answers and Discussions

6.6.1 Discussions on Activity 4

This probably seemed like an easy question, until you tried to write something down. It is important to realize that this type of task is difficult to carry out. To carry it out in a fair manner, we have to be extremely aware of our own prejudices and be self-critical. It would be very difficult to carry outthis type of task without careful consideration of the users' requirements.

6.6.2 Discussions on Activity 5

You might have concluded that there is a wealth of information about Web activities. This information is quite easy to access and it is also quite easy to destroy. We have the ability to control some of the information left on our machines but awareness of how we can do this is required.

These data trails are not always intended to allow activity tracking. History lists allow you to return to a Web page that you forgot to bookmark. Recent document lists allow you to return to tasks that you have been recently engaged in. These facilities are intended to assist us.

6.6.3 Discussions on Activity 6

The difference between the two types of system is in the strategy used to allocate IP addresses. In many company networks IP addresses are allocated either statically, with one machine being given a well-known address which it keeps for its functional lifetime, or dynamically, where a machine may be supplied with a new IP address every time that it boots. If a DHCP server [http://www.dhcp.org/] is used, it is possible to keep records as to which machine is allocated which address.

An ISP must use a DHCP server to supply dynamic IP addresses in order to have more clients than available IP addresses. This means that each time somebody logs into their ISP, their IP address is different, making it very difficult to track Web activity.

It is possible to use software that can disconnect and reconnect to the ISP so that our IP address changes even within what could be considered a single Internet session.

If somebody had access to the ISP server, then it might be possible for them to track changes in the IP address as they occur. This has been used by police to catch criminals.

In Windows you can run software to identify the IP address. Whilst you are connected to the Internet, select the *Start* button, then *run* and type *winipcfg*. This will give you your current IP address.

1. To prevent employees wasting company time accessing material irrelevant to their tasks and to prevent the downloading of material that could compromise the company.

2. Blocking software contains lists of "objectionable" sites, and prevents them from being accessed.

Chapter 7. Property Rights and Software

Table of Contents

7.1 Scenarios

7.1.1 Scenario 1: Pirated Software from Abroad

Bernie works for a large consulting company. When he was on holiday in South East Asia he found an Office suit that looks identical to Microsoft Office. The package he found costs R50 compared to the price tag of R3000 back home. Bernie knew that the seller does not honour US copyright law. Despite the documentation looking like it has been photocopied, he decided to buy it and returned home with it.

Activity 1

Do you think Bernie has done anything wrong? Do you think the customs will confiscate it should they find out? Discuss.

7.1.2 Scenario 2: Stealing an Idea

It is 1980 and Bingo software has just developed a new operating system called BOS. BOS is better than anything else around but Bingo is a small firm and needed venture capitol to start up. It spent 3 years bringing the product to the market, after which it launched and sold well for a year. At this point, it has recovered about 25% of initial investments. Pirate Pete entered the market with PPOS which is cheaper and has more features than BOS – but it appears to be a copied or slightly modified version of BOS. In addition to this, copying of BOS is rampant with customers making copies. Bingo didnot last long and went bankrupt within a year.

Activity 2

Do you think that this is unfair? Has PPOS wronged Bingo? Have the customers wronged Bingo? Discuss.

7.1.3 Scenario 3: Improving Software

Earl develops a virus tester which is very good. It detects and repairs all known viruses. He makes the software and its source code available on the web for free and he also publishes an article on it. Jake reads the article and downloads a copy. He figures out how it works, downloads the source code and makes several changes to enhance it. After this, Jake sends Earl a copy of the modified software together with an explanation. Jake then puts a copy on the web, explains what he has done and gives appropriate credit to Earl.

Activity 3

Discuss whether or not you think Earl or Jake has done anything wrong?

Activity 4

There are some issues that you should think about before proceeding further. Write down any thoughts you might have on each of the following:

- Distinction between hardware and software is often blurred.
- Macro issues – should software be owned? Should it be protected like property?
- Micro issues – are (unauthorised) copies illegal? (Ultimately it will be argued that copying is wrong because it is illegal not because there is some pre-legal immorality involved in the act.)
- Legal and moral issues – descriptive (what the law says) versus normative (what the law should say)

7.2 Some Definitions

- **Algorithm** – abstract method of solution
- **Source Code** – step by step solution to a problem, usually in high level programming language. It is usually created by a programmer employing one or more algorithms.
- **Object Code** – actuates the setting of switches to enable the computer to perform the underlying algorithm

7.3 Current Legal Position

7.3.1 Copyright versus Patent Laws

Consider the Bingo scenario where by PPOS copies BOS and sells it for cheaper. PPOS is able to do that because its development costs were lower. It also seems unfair that PPOS used BOS without paying. What is the solution to this problem? A simple one is to give Bingo legal exclusive right to its software – the problem is then limited to copyright and patent law. This is indeed what happened in the past.

There are currently three mechanisms to deal with scenarios like Bingo: copyright, trade secrecy and patent.

7.3.2 Copyright

Copyright is a form of ownership which excludes others, for a limited amount of time, from copying without permission. Only expression of an idea, and not the idea, can be copyrighted. There is often a fine distinction between the two. In computing, both source and object codes are thought of as 'literary works' and are copyrightable because they are expressions of ideas.

However, there are problematic issues which arise in computing field and not (as much) in others. It is relatively simple to make minor change to a piece of software – making it into a new application. Does this mean that copyright only apply to the old version or just part of the new version that contains the old code? Are copyright owner required to reapply every time a new piece of code is added? This has lead to many course cases. It has been suggested that the literary analogy is not suitable for dealing with software copyright.

Activity 5

Discuss the main difference between software and literature? Apart from the constantly evolving nature of software, what else can you say about software that would make the literature analogy inappropriate?

You can find a discussion of this Activity at the end of this chapter.

7.3.3 Trade Secrecy Laws

Laws governing trade secrecy vary from country to country. The central idea is to grant companies the right to keep certain kinds of information secret (e.g. a secret recipe), with the aim of allowing them to keep a competitive edge. The laws were not designed with computer technology in mind.

In order for a piece of information to be considered trade secret, it be possible to show that:

- It is novel.
- Represents an economic investment to the claimant.
- Have involved some effort in development.
- The claimant has made some effort to keep it secret.

Trace secrecy laws can be applied to software. This is usually done using non-disclosure clauses. Employees sign an agreement that they will not reveal secrets learnt at work even after they have left. There is often ambiguity here because the agreement does not apply to generic information in the area. Another application of this law is via licensing agreements. Software is licensed out and not sold – only the object code, and not the source code, is given to the user. The software company can do all the modification to suit the client and still retain control. The source code is in effect a trade secret.

In Bingo's case, trade secrecy would have helped. Non-disclosure agreements would prevent employee from giving away important secrets even after they left. However, this might only be useful during development; once BOS is released, it is more difficult to control. General principles are there for everyone to see (and copied) – BOS is trying to sell or licence the software, something just can not be hidden. However, specific behind-the-scene methods of doing something can still be made a secret. Generally, trade secrecy works for specialised bespoke software but is poor for general purpose software.

7.3.4 Patent Protection

This is potentially the strongest form of protection because a patent:

- Gives inventor monopoly on use of the invention – even if someone else makes the same product in a different way; they are excluded from using it.
- Grants patent owner the right to licence others to make, sell or use the invention.
- Legitimise a monopoly
- Is granted for a limited number of years (17 in the USA)

The main aim of the patents is not only to ensure inventor, but to advance useful arts and science as well. This will foster inventions and encourage others to learn from and build on inventions. It also promotes disclosure of inventions and assures that ideas already in the public domain remain there.

However, it must be noted that patent does not guarantee financial success. This is only achieved if the product is accepted by the market. Additionally one can not patent an abstract idea, an algorithm or a scientific principle.

To qualify for patent protection, the object in question must satisfy the following criteria:

- Falls into a category of permissible subject matter
- Satisfies the three tests of having utility, novelty and non-obvious.

7.3.5 Software and Patents

In the 1970s, there was great reluctance in granting patent on software on the basis of:

- Fear of ownership of mental process
- Fear of patenting a mathematical algorithm

Both fears have since been overcome. After the US court case of Diamond versus Diehr was settled in 1981, many patents have been granted on software. However, there is still concern that patents must not be granted for building blocks of science and technology.

7.4 Software as Property

Software has challenged the traditional notion of property and ownership. There have been two theories:

- Consequentialist: Property rights are good because they lead to good consequences
- Kantian: Everyone has the right to be autonomous. From this one can derive a right to property (Labour theory of Property)

The idea of natural rights is also applicable. This idea is derived from Locke's Labour theory and states that a person has a natural right to what he/she produces. This can be applied to software as well. Recall the Bingo case. PPOS copied BOS and as such they stole Bingo's labour. Bingo has lost the capacity to sell (and make money from) its creation.

Note: John Locke (1632-1704)

Probably the most famous justification of property in general comes from John Locke, who argued that if one mixed one's labour with something then one had legitimate claim to it. He did, it must be said, place some restrictions on the right to appropriation. There had to be, for example, "enough and as good left for others". The main weakness to this argument is that it is not obvious why we should gain what we mix our labour with, rather than simply losing our labour. John Weckert (1996) illustrates this point:

> *'If I poured a can of tomato juice, which I owned, into the sea, clearly I would not thereby own the sea. I would merely become juice less.'*

There have also been arguments against software ownership. The main point is that ownership of a program leads to ownership of the mental steps that make up the program. If such mental steps are owned then this means that others can not use them and this might interferes with freedom of thoughts (e.g. consider if someone were to 'own' the IF statement). Some people reject this idea because the level of knowledge that was considered is generic and common.

The absence of ownership might also cause bad consequences. Claim has been made that lack of ownership will lead to lack of incentive to produce software. However, software writers are not always in it for the money – consider freeware and shareware.

Activity 6

Find out more about freeware and shareware if you do not know these terms. You can find a discussion of this

Activity at the end of this chapter.

The idea of software ownerships allowed for application of copyright, trade secrecy and patent laws. Together, these encourage invention, innovation, new products and creative invention.

7.4.1 Is it wrong to copy proprietary software?

In general the answer is yes. However, copying might be allowed in the licence in certain including fair use and back-up purposes. In some countries, fair use of the copyrighted material is allowed for the following purposes:

- Criticisms or comments

- News reporting
- Teaching
- Scholarship or research
- Some governmental purposes such as parliamentary or judiciary proceedings and commissions and statutory inquiries.

Fair use of proprietary software is not considered wrong or illegal in most countries. Additionally making a copy to prevent serious harm might also not attract legal consequence in many jurisdictions.

A very philosophical argument puts across the idea that the act of copying software in itself is not wrong because there is nothing intrinsically wrong with the act. It's the act of using the copied software that is the problem. While the person who has been licensed for the software may not have been harmed (copying does not deprive the person of the procession) but the authors are deprived of payment for their labour.

7.5 Fair Use in the Electronic Age

The purpose of this section is to outline the lawful uses of copyrighted works by individuals, libraries, and educational institutions in the electronic environment. Representatives of the following associations advocate the arguments below:

American Association of Law Libraries, American Library Association, Association of Academic Health Sciences Library Directors, Association of Research Libraries, Medical Library Association and the Special Libraries Association.

> *'The primary objective of copyright is not to reward the labour of authors, but "to promote the Progress of Science and useful Arts." To this end, copyright assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by a work. This result is neither unfair nor unfortunate. It is the means by which copyright advances the progress of science and art.'* - US Supreme Court Justice Sandra Day O'Connor

It follows that the benefits of the new technologies should flow to the public as well as to copyright proprietors. As more information becomes available only in electronic formats, the public's legitimate right to use copyrighted material must be protected. In order for copyright to truly serve its   purpose of "promoting progress," the public's right of fair use must continue in the electronic era, and these lawful uses of copyrighted works must be allowed without individual transaction fees.

Without infringing copyright, the public has a right to expect:

- to read, listen to, or view publicly marketed copyrighted material privately, on site or remotely
- to browse through publicly marketed copyrighted material
- to experiment with variations of copyrighted material for fair use purposes, while preserving the integrity of the original
- to make or have made for them a first generation copy for personal use of an article or other small part of a publicly marketed copyrighted work or a work in a library's collection for such purpose as study, scholarship, or research
- to make transitory copies if ephemeral or incidental to a lawful use and if retained only temporarily

Without infringing copyright, non-profit libraries on behalf of their clientele, should be able:

- to use electronic technologies to preserve copyrighted materials in their collections
- to provide copyrighted materials as part of electronic reserve room service
- to provide copyrighted materials as part of electronic inter-library loan service
- to avoid liability, after posting appropriate copyright notices, for the unsupervised actions of their

users

Users, libraries, and educational institutions have a right to expect:

- that the terms of licenses will not restrict fair use or other lawful library or educational uses
- that U.S. government works and other public domain materials will be readily available without restrictions and at a government price not exceeding the marginal cost of dissemination
- that rights of use for non-profit education apply in face-to-face teaching and in transmittal or broadcast to remote locations where educational institutions of the future must increasingly reach their students

Carefully constructed copyright guidelines and practices have emerged for the print environment to ensure that there is a balance between the rights of users and those of authors, publishers, and copyright owners. New understandings, developed by all stakeholders, will help to ensure that this balance is retained in a rapidly changing electronic environment.

The above working statement addresses lawful uses of copyrighted works in both the print and electronic environments.

7.6 Answers and Discussions

7.6.1 Discussion of Activity 5

Most arguments seem to evolve around the fact that a piece of software's behavior in itself is useful, even without the presence of a user. This is not true with literary work.

Another issue is that copyright does not give a monopoly of control of a literary work – someone else, independently can do the same thing. As long as the work was created independently and is literally different there is no copyright infringement. In computing, however, striking resemblance is enough for a court to declare a copyright infringement. Here are some infringement cases:

- Franklin versus Apple (1984): Franklin copied Apple's operating system, in many cases this was done line by line. He was found guilty of copyright infringement.
- Whelan versus Jaslow (1987): Whelan developed a program for Jaslow in Fortran, but both agreed that Whelan would Own it. Jaslow then redid the program line by line in Pascal. Whelan sued and even though Jaslow's program is literally different and arguably a different expression of the same idea, the court found in favour of Whelan (Comprehensive non-literal similarity).

7.6.2 Discussion of Activity 6

Freeware are software which anyone can used without paying the author. People do produce this type of software for fun or just because they want the software themselves. Shareware are software that is provided for use or a trial basis. After the trial period is over, users may pay a small amount to carry on using it and/or for support. They must remove the software from their system if they do not intend to pay.

Chapter 7. Accountability in IT

Table of Contents

7.1 Scenarios

7.1.1 Scenario 1: Virtual Rape

LamdaMoo is a MUD (multi-user dungeon, dimension, or sometimes domain) game, that allows player to create spaces and character and to use them to interact with other players' characters and spaces. Bungle wrote a piece of software that took control of other players' characters and make them do sadistic actions including rape. The actual owner of the character has no control over these actions. As a result, LambdaMooers are outraged and wanted bungle removed. Various opinions have been voiced ranging from expulsion to support because 'he has done nothing wrong'. In the end, the community decided to banish Bungle and to prevent similar incidents in the future, the rules were changed such that any player's characters and spaces can be modified or removed, if the majority of players agrees.

Activity 1

Think about the following questions.

- Did Bungle do anything wrong?
- Consider that he was responsible for the event and that he violated an implied, but not formalised rule. What did he do wrong?
- Do you agree with what the community did? How should he be treated?
- What about the community's new rules concerning what amount to censoring? Do you

think more safeguard is needed? If so, what?

7.1.2 Scenario 2: Designing-making Systems

Kim works for an investment company. Her job is to pick investments for a pension fund. To help her make decision, she uses an expert system. Each upgrade of the system gives more complex analysis.

Kim is very nervous about the market this week. Her personal indicators point to the market going down, while the expert system points to it going up. The system recommends that she puts substantial investments into the market but she does not understand the system's analysis. She also can not judge if the system is defective.

Activity 2

What do you think Kim should do? Should she go with her own analysis and feeling or go with the market. If she makes the wrong choice, she will lose a lot of money for her company. Also consider the following questions:

- Can Kim be held responsible if she uses the information of the program and that turns out to be the wrong decision? Perhaps company should have a policy dealing with situation such as this?

- Can the system's designer or owner be sued or held responsible if the system is working properly? What about if the system is found to be faulty?

7.1.3 Scenario 3: Service Provider for Online Forums

Milo is a freelance journalist and specialises in South American politics. He uses the Internet to keep up to date and uses his computer to write articles, news, as well as taking part in online chat rooms and forums.

He has been away and on his return, eh is outraged to find postings on a forum attacking him. In these postings, it was claimed that he is a drug dealer and that his stories are filled with lies. In response, he posts a denial and also contacts the forum administrator for names and address of the defamer (All posters are required to register with their real names and address for billing purposes). However, the forum administrator refuses to give him this information. Milo is now suing them because he can not sue the perpetrator.

Activity 3

Do you think the forum administrator should be responsible for what is said in the forum? If no, then who should be? What about giving the information away? Recall the relevant privacy issues concerning information collected.

7.1.4 Scenario 4: Y2K Problem

Recall the infamous Y2K problem, where by to save precious memory space year information is truncated to two digits (e.g. 1975 is stored as 75). As the year 2000 approached, calendar dependent activities were at risk. The public reacted to this with disbelief and outrage. Were the professionals asleep? Was it a ploy for companies to employ more professionals and charge their customers to fix this issue? Should the manufacturers and designers have had more foresight? Why was more not done earlier to address the issue? Who should pay for the costs?

However, the year 2000 arrived with no major catastrophe. There were only a few isolated problems. Various opinions have been expressed on this issue – some saying that the problems were fixed on time; while others saying that the problem was over stated. Whatever is the case, who was responsible, and why did this problem actually ever occur?

7.2 Ensuring Accountability

Computer systems are powerful and can cause harm financially, physically or psychologically. To be mindful of this is one of the professional duties identified in most codes of ethics and/or conduct. One approach would be to find appropriate laws and to use them. However, different laws applies in different situations for example, one law might be applicable defective product, while others to negligence. Another factor is the rate of change the technology. Typically it can take a long time to pass a piece of legislation, by which time the technology might have evolved.

In addition to relying on legislation, we can also employ a mix approach in terms of accountability, responsibility, liability and blame. We will discuss these terms individually:

7.2.1 Accountability

This is used in its broadest meaning. It refers to the appropriate agent to response and depends on various factors. For example, in a department in a company, the head of department might be held accountable. Accountability rests with someone with the ultimate responsibility.

7.2.2 Responsibility

There are many types of responsibility:

Role Responsibility: This is analogous to duty. It is what people are expected to do within theirrole. For example, in Scenario 1 with LamdaMoo, players are expected to play by the rules, even if they are not stated. Most players assume that it means not taking over another players' character.

Casual Responsibility: This is a responsibility as a result of causality. For example, X did something and caused an event to happen. Kim invests a large amount of money in the Market and cause the company to lose money, even though Kim might have done all that was required of her duty.

Blameworthy Responsibility: Kim may or may not be responsible, but she is not blameworthy. Perhaps the software was faulty – in that case, the software designer might be blameworthy if s/he failed to fulfil a role responsibility.

7.2.3 Liability

A friend slips on the polished floor of your house and break a leg. You might be held liable but you may not be blameworthy.

7.3 Buying and Selling Software

What are the various responsibilities of the different role players – buyer and seller? The seller:

- Has the right to sell
- Has a duty to be honest
- Has a duty not to coerce a client
- Expected to emphasise the good aspects of the product
- Expected to answer questions honestly

Is a seller being dishonest if they do not disclose a problem area not asked about? This is probably the case but it is very difficult to say especially if the user's needs are varied and complex – how does the salesman know what the needs are. To a naïve user, the answer might be yes, but it is difficult to compel this. Usually, the product itself (either packaging or licence agreement) will contain allthe necessary information. Contract can be voided if all relevant information is not given.

The buyer also has the responsible to find out all the necessary information and ask the right questions if there is lack of it.

7.3.1 Software – Product or Service?

This depends on the circumstances of how the software is produced and/or sold. A comparison can be made between software and buying a suit. (Prince 1980). There are three types:

- Off the peg / Ready to wear (no alteration)
- Tailor made to specific requirements of person
- In between (oo the peg + alterations)

For software a similar groupings can be made:

- Mass market (a product)
- Customised software (service)
- Mixed (Product + service)

7.3.2 Mass Market Products

With mass market, strict liability can be imposed on this type of product. Producers can be sued for errors or malfunctions causing damage because:

- Producers puts the product in the public domain and invites people to buy or use it
- Producer earns profit and should bear the risks
- Producer is in the best position to anticipate and control the risks associated with the product, thus the onus is on the producer to get the product right.
- Producer can spread the cost of injury and insurance over all clients.

The reason for this utilitarian is that placing the onus on the producer has positive effects.

7.3.3 Customised Software

Strict liability does not make sense here as software created and designed specifically for client. The client knows the context in which the software will be used and so specifies what is required. The client thus needs to take part of the risk. This type of software should thus be considered as a service.

7.3.4 Mixed Case

The product and service should be treated each on its own.

7.4 Negligence

Negligence is a failure to do something that is expected of a reasonable and prudent person. For example if a security guard is knocked unconscious, he cannot be blame, but if he is drunk, he might be considered negligent. There is always presumption of a reasonable standard of behaviour. Often this is used to describe blameworthy behaviour of professionals.

The definition of standard applicable to the offence is often quite difficult to arrive at. Often this is best judged by other professionals (conflict of interest issues?).

7.5 Example: Y2K Problem

In the end, companies involved did a lot of checking and spend a lot of money in correcting the problem – resulting in no serious disasters. However, the question of responsibility remains. Who should pay for the cost of upgrading or modifying relevant hardware or software?

- Hardware Manufacturer?
- Company using the computers?
- Computer Professionals who designed the system?
- Professional Society?

- All of the Above?

7.5.1 Who was responsible?

1970: 2 byte data for storing year information saved expensive space – the professionals did a good job.

1980: Same answer

1990: Same answer? Were the systems expected to last for 10 years? What is the cost of storage at this time? What is the cost of upgrading old system?

1995: Same answer? Were the systems expected to last for 5 years? Storage and upgrade cost? Should professionals warn companies of the Y2K problems? Should CSSA have a recommended code of Practice concerning this issue?

1998: Same question, different answer? Client companies all had policies. These were communicated to the shareholders and everyone accepted their responsibilities.

So it has been a lesson. The best strategy is:

- State clearly the role responsibilities of all concerned. Professional needed to explain and document the problem and then to offer options.
- Make sure that all involved understood the effect of their work on humans. Clients needed to understand available options – they needed to realise that the option of staying with 2 digits was short-term and unsafe.
- Hold those responsible who fail to live up to their responsibility.

7.6 Diffusion of Responsibility

In creating a computer system appreciate the following:

- Scale and complexity of the system
- The number of people involved in development, distribution, training and using it.
- What the system will be involved in – many will be involved in important decision making.
- Kant: Humans are responsible for their actions because they have the capacity to control their action.

7.6.1 Example: THERAC-25

THERAC-25 is a computer controlled system that gives radiation treatments to patients. Several patients received massive doses, resulting in at least three fatalities. It was difficult to discover who was responsible, but Therac was liable and paid compensation to the victims' families. Eventually it was found that the action of the operator has caused the accidents. However, it was also found that if an operator entered incorrect mode, noticed this and corrected the error (within 8 seconds as specified), the system still went wrong and the patient was killed as a result. Thus while the operator caused the accident they were not to blame.

The error was traced to also exist in previous version of the software, but had caused no problems because there was only one mode in that version. Was it the designer or the tester (who looks for errors and unconformities to the requirements) who was at fault? The Therac case also illustrates the difficulty of testing real-time systems. Should there have been a feature on the system limiting the radiation dose to some MAXIMUM irrespective of everything else. If so, should this not have been specified by the clients? Are they also partially to blame?

7.6.2 Example: ISP Responsibility

Recall the scenario with Milo, a service provider provides him with chat rooms and forums facilities. Milo was defamed by another user and has the right of recourse. The obvious route to deal with this is the hold the individual responsible – the problem is that the individual is anonymous.

Stratton versus ISP Prodigy (1995)

Prodigy was sued by users with respect to content in its online forums which Prodigy has advertised that it has editorial control over. The court has applied the law governing newspapers and found Prodigy guilty. However, Prodigy claimed that they were like a telephone company and not newspaper company. The following year, the US Communications Decency Act reversed this on the basis that ISPs are closer to telephone companies. The act also introduced the Good Samaritan immunity in which an entity can exercise control without liability and is encouraged to do so.

7.6.3 Example: Virtual Action

Consider the first scenario involving rape in cyberspace. Bungle raped no real person but has upset the other participants. However, he did abuse a new form of expression to expose other people to pornography and violence without their consent. He violated an unwritten rule of the MUD game – sort of like stealing money in a game of Monopoly.

It is tempting to think that because it is a game, his behaviour is not real. This thinking maybe appropriate when considering flight simulators but when the actions involved real people, one should consider

- Consequences (financial, physical and psychological) to others.
- One’s actions have effects on others.
- That one can be mediated by technology.
- Can claim that virtual environments are not morally neutral – one’s behaviour in the virtual environment is real.

In effect, Bungle:

- Violated his role responsibility as a participant in the game.
- Is causally responsible for participants witnessing violence etc.

The issues of blameworthiness and liability are complex. He has broken rules without seeking consent. While virtual environments can allow people to do real and useful things such as in education and medicine, it can also create complex issues when dealing with responsibility – as has been seen in the virtual rape scenario. Consider a case of a medical doctor performing surgery via remote access.

Midway through a complex procedure, the link is lost and the patient dies. Who should be held responsible? How would you start investigation into this issue? The key is to start by identifying role players and their responsibilities, then look into the issue of blameworthiness and liabilities.