Professional Practice & Ethics

Computer Science Tripos Part IA

Dr. Richard C. Jennings
Department of History and Philosophy of Science
University of Cambridge

Contents

Ethics — an introduction..... 1
I Professional practice..... 3
II Computer cracking 7
III Data privacy 11
IV Software & property..... 15

Ethics - An Introduction

Introduction - Basic Questions

There are three basic questions in ethics: “What are the true moral values?”, “How do we know, or discover, them?”, and “How do we justify them?” or, “Why should we act morally?”. Many different theories have been offered in the attempt to answer these questions. They can be grouped into five main kinds: authority theories, intuitionist theories, egoist theories, consequentialist theories, and deontological theories.

I. Authority Theories

Authority theories are typically held in a religious context where ethics are based on a set of scriptures, theological interpretation of the scriptures, or a priesthood who are regarded as competent in interpreting the scriptures. In general the idea is that what is good is what God says is good. In practice, however, we depend on a representative of God to tell us what is good because God rarely gets directly involved in such tasks.

The main difficulty with ethics based on authority is that we can imagine the Authority telling us to do something like killing those who you don’t like. If we feel that the authority would not tell us to do bad things, then it is clear that we have another criterion of good and bad.

II. Ethical Intuitionism

Because ethical characteristics of actions cannot in any obvious way be identified with their other physical characteristics, nor are they obviously definable in terms of those characteristics, some philosophers have argued that ethical characteristics are a non-physical, but nonetheless real, characteristic of actions. They argue that ethical characteristics can be seen immediately in the same way that we can see that something is green, or large.

The main practical difficulty with intuitionist theories is that, unlike authority theories, there is no way to resolve differences of opinion. If I see that an act is good and you see that it is bad, there are no further considerations to help decide who is right. Ethical Intuitionism does not allow for resolution of conflict - ethical judgement is completely subjective, if I think something is good and you think it is bad, that is just a difference of judgement, there is no further fact of the matter.

III. Egoism

Egoist theories hold that what is morally right derives from our own self-interest. Since our most basic inclination is to look after ourselves, it seems that few could dispute an ethical theory based on that. Psychological egoism is the view that all our actions are in fact motivated by self-interest.

But this is a descriptive theory not a prescriptive theory - it claims to describe how we do behave rather than how we ought to behave. Ethical egoism introduces the prescriptive force, the ought, into egoism. One version is based on two credible premises: 1) It is rational to act in our own self interest, and 2) We ought to act rationally. If we accept the two premises, then we ought to act in our own self interest.

There are two main problems with egoist theories. First, like intuitionist theories, they do allow for conflict resolution; and second they do not take into account our fellow feelings, our feelings of sympathy and commiseration.

IV. Consequentialist Theories

Consequentialist theories are theories that determine moral values on the basis of their consequences. But the consequences are not confined to consequences for oneself, they include consequences for everyone.

A. Utilitarian Theories and others

According to utilitarian theories we ought to do things which maximize pleasure or happiness for everyone, or, at least we should not interfere with people doing what gives them pleasure as long as it does not detract from the pleasure of others. A problem with this view is that not everyone makes pleasure or happiness their major goal. A more sophisticated version would aim to maximize satisfaction of preferences. But, even so, some people's preferences are not in their long term interests - children's food preferences, or drug addicts' preferences, for example.

B. Problems with Consequentialist Theories

There are a number of problems with consequentialist theories. First is the need to justify the basic claim that we ought to maximize pleasure (or happiness, or satisfaction of preferences). Second, there are real practical difficulties in quantifying happiness (or whatever). Third, there is no end to moral considerations - since every act has consequences, everything we do needs to be considered from a moral point of view. Fourth, such theories can lead us to treating certain individuals very badly if the total happiness is greater than their unhappiness.

V. Deontological Theories

An alternative way of answering the three basic ethical questions is to start from a consideration of what our duties are - irrespective of the consequences. One possible way of discovering our duties is through reason. Another is through considering our role in the social order.

A. Reason Based Theories

1. Natural Rights

In a state of nature we are free to do whatever we want. Some of these freedoms we can agree to compromise in the interest of social accord, but others are too basic to compromise. The freedom to gather in groups and to speak together, for example, are necessary to achieving such agreements and social accord and therefore cannot be compromised. Other freedoms, such as the freedom to take what we want from what we see around us or the freedom to kill those whom we don't like, can be given up in the interest of social accord.

2. Kant

Kant argued that some moral principles were rational. Kant's ethics is based on the 'Categorical Imperative': Act only on the maxim which you can at the same time will to be a universal law. This principle can be used to justify the principle of telling the truth because if we considered the principle 'lie when it is convenient' the institution of truth-telling would collapse and it would no longer be possible to lie.

B. Social Order Theories

An increasingly popular method for determining and justifying moral values is to consider what principles contribute to a fair and harmonious social order.

1. Egoistic Contract Theory

From the egoistic point of view it is in our own interest to make some agreements with other people around us to refrain from certain kinds of actions like stealing and killing. But this morality depends on an equal distribution of power - if we can act against others and prevent them from acting against us, then there is nothing immoral in acting against them.

2. Rawls' Theory of Justice

Social contract theories suppose that our duties are determined by an agreement that we make with others in order to further our own personal goals. But in fact we are born into an existing social practice. For John Rawls the justice of a given practice can be analyzed by considering whether we would be satisfied to be born into any role in that practice. We may wonder if it is really possible to put aside our interests and look at a social practice through a "veil of ignorance".

I Professional Practice

Modern computing science is an esoteric body of knowledge which is universally used and almost universally opaque. The computer scientist is in the position of providing for the general public a service which is taken on trust. In the public domain there is very little DIY computing because the effort and especially the knowledge needed to create or modify computer systems is beyond the capacities or interests of most users. In a word, the computer scientist provides a service which must be taken on trust and which, in the late 20th Century, is essential to public life.

A. What constitutes a profession?

The law society defines a profession as follows:

> When a profession is fully developed it may be described as a body of men and women
> (a) identifiable by reference to some register or record;
> (b) recognized as having a special skill and learning in some field of activity in which the public needs protection against incompetence, the standards of skill and learning being prescribed by the profession itself;
> (c) holding themselves out as being willing to serve the public;
> (d) voluntarily submitting themselves to standards of ethical conduct beyond those required of the ordinary citizen by law
> (e) undertaking to take personal responsibility to those whom they serve for their actions and to their profession for maintaining public confidence.

Modern professional codes of ethics cover more relationships than the two basic ones covered by the hippocratic code. In general they also include relationships between employees and employers and between the professional and the public in general.

B. Professional Relationships

1. With employers

a. Loyalty

In general employees are expected to show loyalty to their employers - they are expected to recognize and help the employer achieve her ends. But there are limits to loyalty, for example the employee must retain the right to support the political party of their choice without threat of job

loss, and they must not be expected to buy only company products, in preference to the competitor's.

b. Trade secrets

In a free labour market it is difficult to protect trade secrets. A company can afford to hire a competitor's employee at a higher price than the competitor if the employee carries information that gives the company a market lead over its competitor. Companies attempt to guard against this practice in several ways. Employees can be asked to sign agreements promising not to reveal trade secrets. They can even be expected to agree not to work in the same industry for a set period after they leave a company. There is a moral sense in which loyalty should carry over beyond the term of employment.

2. With clients

There are roughly three ways the relationship can be seen and it is necessary for a smooth running relationship that there be some agreement about what sort of relationship it is. Essentially the difference concerns the balance in decision making between the company and the client. If the company is seen as the agent of the client, it simply carries out the client's wishes, it does not make any significant decisions of its own. When it has to make a decision about aspects of design that are not obvious from the client's wishes, then it must return to the client for clarification. This is the agency model. At the other extreme, the client may transfer all the decision-making authority into the hands of the company. In this case the company first learns as much as it can about what the client wants and then, during the process of development, makes all the decisions about how best to realize the client's desires. This latter is the paternalistic model. In between these two extremes an interactive model where the client is engaged in making decisions but is advised by the company. The decisions are not entirely the client's, nor are they entirely the company's. Decisions are arrived at through a process of dialogue in which the client expresses her wishes and desires and the company advises on what is possible from a practical and what is advisable from their own point of view of superior experience.

3. With the public in general

The obligation of the professional to the public at large can be seen as a kind of implicit contract that the professional makes with society to allow him, and not just anyone, to practice his trade. Society in general, through its legal system gives the professional the right to maintain a monopoly in the practice of his profession, on the understanding that the professional will act for the good of society.

4. With other professionals

A popular image of the professional organization is that its sole purpose is to promote the interests of the professionals themselves. It is like a monopoly of practitioners who have managed to corner the market and convince the establishment that they have some special skill that no-one else has. Thus they manage to legalize their particular monopoly and squeeze out any other practitioners. Once organized they can set their own fees and standards of performance. One has only to recollect the legal profession as portrayed in Charles Dickens' *Bleak House* to get the image.

But even with such a cynical view of the professional organization, there is reason to suppose that it is in the interest of the profession to adopt some controls on the behavior of their members. An individual who does not act in the interest of the client will damage the reputation of the profession as a whole. And when the trust that people place in the profession is damaged, the people will begin to look for alternative sources of expertise - they will turn to alternative medicine, or begin to practice their own conveyancing.

C. Codes of Professional Ethics and Conduct

1. History

The first professional code of conduct was the Hippocratic Oath taken by physicians in ancient Greece. The first such code in the UK was a code of medical ethics drawn up by Tomas Percival in 1803. Between 1870 and 1910 many professional institutes of engineering and applied science incorporated codes of ethics into their professional statutes. between 1910 and 1960 there was little increase in the number of such ethical codes adopted by professional organizations, but between 1960 and 1989 the number of codes of conduct, or ethics, adopted by professional bodies increased by about a factor of ten.

2. The First Code of Ethics: The Hippocratic Oath

Rules governing the relations between members of a profession are aimed at maintaining the integrity and continuity of the profession, and minimizing conflict or competition between members of the profession. Rules governing the relations between the members of the profession and their clients, the public, are intended to ensure continuing public confidence in the profession and thus to maintain public use and support for the profession.

3. BCS Code of Conduct[1]

Introduction

This Code sets out the professional standards required by the Society as a condition of membership. It applies to members of all grades, including students, and affiliates, and also non-members who offer their expertise as part of the Society's Professional Advice Service.

Within this document, the term 'relevant authority' is used to identify the person or organisation which has authority over your activity as an individual. If you are a practising professional, this is normally an employer or client. If you are a student, this is normally an academic institution.

The Code governs your personal conduct as an individual member of the BCS and not the nature of business or ethics of the relevant authority. It will, therefore, be a matter of your exercising your personal judgement in meeting the Code's requirements.

Any breach of the Code of Conduct brought to the attention of the Society will be considered under the Society's disciplinary procedures. You should also ensure that you notify the Society of any significant violation of this Code by another BCS member.

The Public Interest

1. You shall carry out work or study with due care and diligence in accordance with the relevant authority's requirements, and the interests of system users. If your professional judgement is overruled, you shall indicate the likely risks and consequences.

- The crux of the issue here, familiar to all professionals in whatever field, is the potential conflict between full and committed compliance with the relevant authority's wishes, and the independent and considered exercise of your judgement.
- If your judgement is overruled, you are encouraged to seek advice and guidance from a peer or colleague on how best to respond.

2. In your professional role you shall have regard for the public health, safety and environment.

- This is a general responsibility, which may be governed by legislation, convention or protocol.
- If in doubt over the appropriate course of action to take in particular circumstances you should seek the counsel of a peer or colleague.

---

1 Online at <http://www.bcs.org/conduct>.

3. You shall have regard to the legitimate rights of third parties.

- The term 'third Party' includes professional colleagues, or possibly competitors, or members of 'the public' who might be affected by an IS project without their being directly aware of its existence.

4. You shall ensure that within your professional field/s you have knowledge and understanding of relevant legislation, regulations and standards, and that you comply with such requirements.

- As examples, relevant legislation could, in the UK, include The UK Public Disclosure Act, Data Protection or Privacy legislation, Computer Misuse law, legislation concerned with the export or import of technology, possibly for national security reasons, or law relating to intellectual property. This list is not exhaustive, and you should ensure that you are aware of any legislation relevant to your professional responsibilities.
- In the international context, you should be aware of, and understand, the requirements of law specific to the jurisdiction within which you are working, and, where relevant, to supranational legislation such as EU law and regulation. You should seek specialist advice when necessary.

5. You shall conduct your professional activities without discrimination against clients or colleagues

- Grounds of discrimination include race, colour, ethnic origin, sexual orientation
- All colleagues have a right to be treated with dignity and respect.
- You should adhere to relevant law within the jurisdiction where you are working and, if appropriate, the European Convention on Human Rights.
- You are encouraged to promote equal access to the benefits of IS by all groups in society, and to avoid and reduce 'social exclusion' from IS wherever opportunities arise.

6. You shall reject any offer of bribery or inducement.

Duty to Relevant Authority

7. You shall avoid any situation that may give rise to a conflict of interest between you and your relevant authority. You shall make full and immediate disclosure to them if any conflict is likely to occur or be seen by a third party as likely to occur.

8. You shall 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 at the direction of a court of law.

9. You shall not misrepresent or withhold information on the performance of products, systems or services, or take advantage of the lack of relevant knowledge or inexperience of others.

Duty to the Profession

10. You shall uphold the reputation and good standing of the BCS in particular, and the profession in general, and shall seek to improve professional standards through participation in their development, use and enforcement.

- As a Member of the BCS you also have a wider responsibility to promote public understanding of IS - its benefits and pitfalls - and, whenever practical, to counter misinformation that brings or could bring the profession into disrepute.
- You should encourage and support fellow members in their professional development and, where possible, provide opportunities for the professional development of new members, particularly student members. Enlightened mutual assistance between IS professionals furthers the reputation of the profession, and assists individual members.

11. You shall act with integrity in your relationships with all members of the BCS and with members of other professions with whom you work in a professional capacity.

12. You shall have due regard for the possible consequences of your statements on others. You shall not make any public statement in your professional capacity

unless you are properly qualified and, where appropriate, authorised to do so. You shall not purport to represent the BCS unless authorised to do so.

- The offering of an opinion in public, holding oneself out to be an expert in the subject in question, is a major personal responsibility and should not be undertaken lightly.
- To give an opinion that subsequently proves ill founded is a disservice to the profession, and to the BCS.

13. You shall notify the Society if convicted of a criminal offence or upon becoming bankrupt or disqualified as Company Director.

Professional Competence and Integrity

14. You shall seek to upgrade your professional knowledge and skill, and shall maintain awareness of technological developments, procedures and standards which are relevant to your field, and encourage your subordinates to do likewise.

15. You shall not claim any level of competence that you do not possess. You shall only offer to do work or provide a service that is within your professional competence.

- You can self-assess your professional competence for undertaking a particular job or role by asking, for example,
    i. am I familiar with the technology involved, or have I worked with similar technology before?
    ii. have I successfully completed similar assignments or roles in the past?
    iii. can I demonstrate adequate knowledge of the specific business application and requirements successfully to undertake the work?

16. You shall observe the relevant BCS Codes of Practice and all other standards which, in your judgement, are relevant, and you shall encourage your colleagues to do likewise.

17. You shall accept professional responsibility for your work and for the work of colleagues who are defined in a given context as working under your supervision.

II Computer Cracking

Hacking and Cracking

Initially 'hacking' referred simply to people who worked with computers, who did the tedious hack work of writing out programmes in machine language. The term came more generally to mean those who enjoyed playing with computers and trying out new things. As the field of computing developed the term began to refer more to people who were able to get the computers to do the unexpected - who pushed at the limits of what computing was all about. In the early days, hackers were just people who were really enthusiastic about computers.

The term hacker still refers to computer enthusiasts, but, because of malicious programmes (viruses, worms, trojan horses, time bombs, etc), it has, in the press, come to mean something more sinister. Computer hackers are still pushing the limits of what computers can do, but in popular terminology they are also breaking conventional limits of what is acceptable. The term hacker is used in many senses. *The Hacker's Dictionary* lists at least seven definitions, among which are the following four:

1. A person who enjoys learning the details of computer systems and how to stretch their capabilities - as opposed to most users of computers who prefer to learn only the minimum amount necessary.

2. A person who programs enthusiastically, or who enjoys programming rather than just theorizing about programming
3. A person who is good at programming quickly.
4. An expert on a particular program, or one who frequently does work using it or on it.

But the popular meaning that is attached to 'hacker' more often means an individual involved with the unauthorized access of computer systems by various means. Or, alternatively, hacking can be defined as any computer-related activity which is not sanctioned or approved of by an employer or owner of a system or network. A further aspect of the popular conception is that the hacker is not into hacking for criminal gain. That is, hacking is distinguished from more serious computer crime. Also hacking is distinguished from piracy which is the illicit copying of software, the unauthorized copying of copyrighted software. For our purposes though we will use the term "cracker" to refer to anyone engaged in unauthorized entry or use of computers. We will leave the term hacker to carry its traditional meaning.

A. Computer cracking - some arguments

Given the rather ambiguous public image of computer cracking, we need to ask about the ethics of cracking. Is it a glamorous Robin Hood sort of activity as some would have it, or is it thoroughly wrong as others would have it? Let us consider some of the arguments that have been offered in defence of cracking.

1. All information should be free

One of the strongest arguments is that all information should be free, which has as a corollary that there would be no problem of intellectual property and security if it were. But of course the problems of intellectual property and security do arise because information is *not* free. So we must ask what grounds there are for saying that all information *should* be free. The basic claim is that in all aspects of our lives we need information. In deciding whether to dress for a balmy day or a cold rainy day, or in deciding whether to go into computing or into mechanical engineering, we need to know things like the weather report or the job prospects in different fields. Moreover, our very political system depends on freely accessible information. If we knew nothing of the candidates in elections, or if we only knew how wonderful one of them was, we would not be able to make a reasonable choice when we came to vote.

The flaw of this line of reasoning is that it doesn't apply to *all* information. Certainly we need to know about the candidates in an election, and we need to know much about the world to make decisions about what to do, both in the short term and in the long term. But there are other things that we value, or at least our society values, which are inconsistent with total freedom of information. Three kinds of information in particular are probably best not made freely available.

a. Capitalism and information value

Without the possibility of keeping trade secrets, the competitive spur to technological development would break down and, it can be argued, so would our economic system.

b. National security

Certain kinds of information are best kept secret for the proper functioning of the government. Public figures attract considerable attention, not all of it positive. If the daily movements of such figures were public knowledge that would be a temptation for people with grudges or extraparliamentary political views.

c. Individual privacy

Finally the rights of individuals to keep certain kinds of information to themselves, or at least within their control, is a well recognized right that we generally would be loathe to give up.

2. Break-ins are beneficial by revealing security flaws

Another argument that is used to defend cracking is that it is a way of revealing the flaws in computer security systems. The cracker is seen as performing the valuable service of discovering weaknesses in the systems that are supposed to limit access to authorized users.

But there is a more sinister problem with cracking. It is this. Typically cracking is not an individual activity, in general cracking is a cooperative activity practiced by groups of people who are linked through computer networks. They share techniques and knowledge with each other and often number among their members individuals who are "insiders" of different systems. In keeping with cracker ethics these networks of crackers are open networks. And the serious problem is that they are open also to those who would use the craft, knowledge and techniques of the crackers for more sinister ends, such as embezzlement and other sorts of computer crimes.

3. Cracking is not harmful and is educational

As for the reputed educational aspects of cracking, it seems clear that there are better ways of learning computing than cracking. The usual methods of reading, listening to lectures, solving problems, and working through learning programmes provides a much broader and more systematic kind of knowledge than the esoteric knowledge of specific details that the cracker needs. Even if cracking did provide a good education, that good would have to be balanced against the harm that is created by promoting the culture of cracking.

B. The Response to Cracking

So far the argument has been that computer cracking cannot be morally justified. But cracking remains an activity glamourized by the media, a challanging activity for the computer puzzle solver, and for many a source of social contact. The question remains as to what should be done about cracking.

1. Social Attitudes and Conventions

The computing world is still a fairly new world and behavioural conventions have not yet been firmly established. We are still in a position to decide whether the conventions of the computing world will be those of good neighbours or those of a state of nature where we take what we can get when we get the chance. Our image of the cracker has a lot to do with what kind of computing world we live in. If we see the cracker as a kind of snoop or benign burglar who goes around the neighbourhood trying to get into the houses, and when he does get in he goes through the drawers and papers just to see what is there, then we have a better chance of making a neighbourly world than if we see the cracker as a kind of Robin Hood figure taking on the computer systems of large corporations or government departments.

2. Education

From their earliest years in school children are now being introduced to computers. If children are introduced to the ethical principles of computer use at these early stages, the principles will become a part of their attitude and conduct within the world of computing.

3. Professional conduct

In the UK, the British Computer Society does not have any explicit provisions against illegal entry into computer systems. The third rule applying to public interest is that members know and understand relevant legislation, and this includes the Computer Misuse Act of 1990 which covers cracking. In other words, the BCS leaves control of cracking in the public sector.

4. Legislation

In spite of the best examples of neighbourly behaviour, and efforts to educate new users in appropriate conduct in the world of computers, there will still be those who persist in violating the conventions of good conduct. And of course there will be the criminal element - those who hope to make financial gains through the techniques of cracking. For this reason various kinds of legislation have been enacted which criminalizes cracking. In the U.K. this has been done in the The Computer Misuse Act of 1990.

a. The Computer Misuse Act of 1990

On 10 October 1989 the Law Commission recommended legislation on the problem of computer abuse. Their recommendations were essentially adopted in the *Computer Misuse Act 1990*, which became law in June 1990. The law creates three new offences:

I. Unauthorised entry into a computer system, with a maximum penalty of £2,000 fine or six months' imprisonment (the Law Commission suggested a maximum penalty of three months imprisonment)

II. Unauthorised entry with intent to commit or assist in serious crime, with a maximum penalty of five years' imprisonment and an unlimited fine (the Law Commission suggested a maximum penalty of five years' imprisonment)

III. Altering computer-held data or programs without authorisation, also with a maximum penalty of five years' imprisonment and an unlimited fine (the Law Commission again suggested a maximum penalty of five years' imprisonment)

Two extensions of this basic law should be noted:

A. The law is extended to cover those who conspire with others to break the law and those who incite others to break the law.

B. The law applies to any violation of the law which has a significant link in the UK. For example misusing a computer in Italy through an ftp connection in the UK is breaking the law. Also if the culprit is not in the UK but accesses the Italian computer through a link in the UK they are guilty of breaking this law.

b. New legal concepts

Apart from the question of illegal entry, there is another consideration that has led to the formulation of new laws governing computer use, or misuse. This is that the traditional laws of Theft, Malicious Damage and so on do not clearly cover the analogous crimes in the computing world. Computing space, cyberspace, is different to ordinary space - trespass normally means physical entry into someone else's space, theft normally refers to the removal of some physical object, breaking into a property involves physically attacking and damaging a lock. The language used in formulating earlier laws is ambiguous when applied in cyberspace. The integrated use of computers is likely to continue and develop and the realm of cyberspace is bound to develop in its own way - traditional legal concepts are not always going to clearly fit our understanding of cyberspace.

5. Institutional Safeguards

Whatever attitudes and laws might be in place to guard against computer cracking, there will still be those who find it a challange, and others who can use the craft of cracking as the basis for criminal activity. For this reason technical security - passwords, encryption, etc. - will be needed to protect sensitive information. But such security will have no value if institutional safeguards are not in place. There are two aspects of institutional safeguarding that require attention. The first is the

institutional structure - There should be clear rules about who has access to what information and the responsibility for access should be well defined. The second is institutional control - once the institutional structure is in place it should be adhered to, those with access to sensitive information should know what their responsibilities are and should take care that the security of the system is not compromised through neglegence on their part.

III Data Privacy

A. Is there a real problem of privacy in data processing?

In contemporary society there is a growing concern that the use of computer data systems may undermine, or "invade", our privacy. Through the use of computers, information about us as individuals is more widely collected, stored, and available, and more easily combined, collated and processed. This means that if there were no controls on the collection distribution and use of personal information, anyone with access to a network terminal could build up a very detailed profile of our life and activities. The invasion of privacy that results from advances in data processing is not simply a change in the degree of privacy; it is a change in the nature of privacy. The data processing invasion of privacy concerns *information* about us, not the openness of the various situations, events and activities in our lives.

One approach to the problem is to argue that there is not really a problem, that we are just worried by the change in information availability. Two arguments are used to support this view, one is that as long as we haven't done anything wrong, it will not matter what is known about us. The other is that if we do not want information about us to be collected we do not have to make it available. The first argument is that privacy is only needed by those who have done something wrong - if we have nothing to hide we have no fear of the data processing invasion of our privacy. But this overlooks the fact that the input to computers is a human process and that errors can occur. Moreover, information that may be irrelevant to a decision about someone may be taken into consideration because it is available. The second argument, that we do not have to provide information to the information collectors is nearly true but only so at a price. If we want to keep our money in an bank or building society we provide personal information. In obtaining a credit card we also supply personal information, and then every time we use the card there is a record of where and how we used it.

B. Personal privacy - what is it?

1. Secrecy?

Because in some situations privacy involves withholding information about ourselves, we may be tempted to think that secrecy is an essential feature of privacy. But secrecy involves actively withholding information and privacy may simply involve retaining information. We do not tell everyone everything about ourselves, that would be boring. But neither do we regard all that information as secret. Just because information is private does not mean it is secret. Nor is secret information necessarily private. We may be party to state secrets, or to business secrets, that are shared by a large number of people. These secrets are not private, but they are nonetheless secrets. Secrecy and privacy overlap when they require conscious supression or hiding of information, but we can have secrets that are not private and we can be private about things that are not secret.

2. Anonymity?

One suggestion about privacy is that it consists in anonymity - as long as we are not known by name any information about us will not affect us, thus our privacy is preserved. But our names are only of use if there is a databank which connects information with our names. And anyway we

wouldn't share some information even if we remained nameless. Maintaining anonymity may be a way of maintaining privacy, but it is not the same.

3. The private vs. the public sphere

Another idea about privacy is that it is a characteristic of certain kinds of information about us, it assumes that there is a sphere of private knowledge and a sphere of public knowledge. So, for example, our name, our sex, our accent, and so on, are part of the public sphere while our sexual inclinations are part of the private sphere. If we think about it there is virtually nothing about us that is not known by someone in our lives. But one important feature of this fact is that we know in general who knows what about us. Privacy is not so much a personal matter as a matter of social relations.

4. Privacy as control of personal information

In 1978 the British government Lindop Committee reported on their investigations into the field of data protection and as part of that considered the question of data privacy. For them the concept of data privacy referred to the individual's claim to control the circulation of data about himself. But information about me can circulate in normal and non-invasive ways without my control. The sharing of the information is partly controlled by the individual, but much of it is not. Privacy is preserved as long as it is distributed in legitimate ways along legitimate channels of social relations.

5. Privacy: an aspect of social relations

It seems paradoxical to think of privacy as an aspect of social relations. But we have seen that nearly everything about us is, or could, be known by someone. It is just that some things are appropriately known by some people, and other things appropriately known by other people. The sort of thing that is appropriate for a person to know depends on the kind of relation they bear to us, the role they play in our lives. A person's privacy does not consist in a particular batch of information (the private sphere) that they keep to themselves, nor does it consist in being in total control over the distribution of information about themselves. Rather it consists in that information being appropriately distributed over the network of social relations in which that person is involved. Privacy is violated when information is distributed in a way that is not appropriate to those social relations.

C. How can we protect privacy?

If privacy is violated when personal information is distributed through inappropriate channels, then what principles should we adopt to prevent this? One principle we could adopt is that:

1. The recipient of personal information must have a legitimate use for it.

This principle limits the collection of information to what is appropriate to the circumstances. The concept of legitimate use for information plays an important part in this principle. We need to state more explicitly what it is to have a legitimate use for information. This is done by a second principle:

2. The purposes of the recipient in acquiring the information must be connected in a positive way with the interests of the subject of that information.

In other words we should consider whether the subject of the information would want to have the information passed along to the recipient. Now obviously some such transfers of information are not in the interests of the individual, but still serve some greater interests. The criminal does not have a right to privacy about his criminal activities because he does not have a right to act criminally. However, there is a balance that needs to be maintained here. The police cannot be allowed free and easy access to all information on everyone. There must be some limits on their powers to access confidential files, just as they have some rights to access files. The fact that

different files have different degrees of confidentiality suggests a third principle to maintain the balance:

3. The availability of personal information must be inversely related to the degree of confidentiality under which it was originally obtained.

And finally, as a control on the distribution of data, a way of ensuring that the second principle is maintained, we can adopt a fourth principle:

4. The subject must have some practicable means of discovering what information about him or her has been transmitted to whom, and must have access to it.

These principles are aimed at preserving the right of privacy in a world where information can easily be gathered, stored and transmitted. They do not preserve an absolute right to privacy, but they assume the right in the absence of some overriding factor. Justification is needed for the acquisition of information, not for the protection of it. The assumption is that information should not be transmitted unless there is good reason to do so.

D. Official Guidelines and Legislation

Having arrived at some moral principles, we can now look at privacy legislation and see how these principles are implemented. In 1980 the Organization for Economic Co-operation and Development (OECD) published *Guidelines on the Protection and Privacy of Transborder Flows of Personal Data*. The guidelines set out eight principles for the protection of privacy in data collection, handling and distribution. The guidelines were adopted by all 24 OECD member countries and provided the foundation for the United Kingdom Data Protection Act of 1984, the "DPA". The DPA of 1984 is due to be superseded in March 1999 by the DPA of 1998, which is intended to bring UK legislation into closer alignment with European legislation. Currently registered personal data processors will be allowed a transitional period of up to two years to bring their operations in line with the European principles. The following are the eight principles of the 1998 DPA.[2] Most of the principles are self explanatory, but the first and sixth principles require some unpacking.

1. First Principle (principle of data gathering)

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -
a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

The basic condition for a) is that the subject has given consent for their data to be processed, but there are a number of exceptions such as processing that is required for performance of a contract to which the subject is party, and processing that is required by the government. The "sensitive personal data" of clause b) includes data on such things as the racial or ethnic origin of the data subject, their political opinions, their religious (or similar) beliefs, their sexual life, and their criminal record.

Under the DPA of 1998 the subject must at least actively consent to having personal data gathered (e.g., failure to return or respond to a leaflet does not count as consent) and where the data is more sensitive they must explicitly consent to having the data processed (i.e., write it down).

The First Principle also subsumes two other important aspects of personal control of data - the right of the data subject to know what personal data is being gathered (the old OECD openness

2 http://www.legislation.hmso.gov.uk/acts/acts1998/80029--l.htm#sch1

principle) and the uses to which that data is being put (the old OECD purpose specification principle).

The OECD purpose specification principle appeared as principle 2 of the UK DPA of 1984. In the DPA of 1998, purpose specification is included in the principle of fair and lawful processing. In particular, this first principle contains a fair processing code which specifies the information to be provided to data subjects. In addition to the identity of the data controller, the data subject must be told the purpose for which the data are to be processed. But the requirements do not stop here - the data subject must also be informed of the likely consequences of such processing and especially whether disclosure of such information can reasonably be envisaged. In particular the data processor is obliged to inform the subject of consequences of processing that the subject may not forsee.

The OECD openness principle held that the data subject should be able to determine the whereabouts, use and purpose of personal data relating to them. The availability of this kind of information creates its own problems of security. We can imagine files which hold personal data about individuals who do not object to having that data held, but who would object to other people knowing that that data is held. For example, police records, or hospital records of people who are HIV positive, or building society records of people who have had to renegotiate their mortgages because of financial hardship. In such cases it would be a breach of privacy if someone else could discover the whereabouts, use and purpose of personal data relating to them. A central register of individuals and the files which included them would then itself require a high degree of security and pose a potential threat to privacy. For this reason no central register is kept, and the openness principle is reduced to the rights of data subjects covered by the sixth principle.

2. Second Principle (principle of data purpose)

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Third Principle (principle of data quantity)

Personal data shall be adequate, relevant and not excessive in relation to the purposes or purposes for which they are processed.

4. Fourth Principle (principle of data quality)

Personal data shall be accurate and, where necessary, kept up to date.

5. Fifth Principle (principle of data lifetime)

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Sixth Principle (principle of data subjects' rights)

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The first right of the data subject is to be told by any data processor if their own personal data is being processed and, if it is, to be told in an intelligible manner what that personal data is, the purposes for which it is being processed, and to whom the personal data may be disclosed.

The data subject also has the right to prevent processing for purposes of direct marketing or where the processing is likely to cause damage or distress, and the data subject has the right to seek a court order requiring the data controller to rectify, block, erase or destroy inaccurate data.

Finally, the data subject has the right to seek compensation for any damage or distress that may result from contravention of the act.

7. Seventh Principle (principle of data security - internal)

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Eighth Principle (principle of data security - external)

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The act is enforced through the office of the Data Protection Commissioner (DPC) who maintains a register of data collectors and processors. Individuals and organizations who regularly process personal data are legally obliged to register themselves with the DPC. They must state what kind of data they are processing and for what purpose they are using it. They are breaking the terms of the DPA if they use the data for any other purpose than what is stated. In addition to the penalties that may have to be paid to individuals if damage is done through misuse of personal data, the data processor can be struck off the register of data collectors and processors. If he is struck off the record then it is illegal for him to store or process any electronic personal data.

IV Software and Property

Ownership of software is, like many issues in the computing sciences, still open to discussion and development. As in other areas of computing, traditional legal structures do not neatly fit the needs and problems of the community. This means that there is room for development in the concepts of property and ownership as they apply to software. Developing these concepts requires an understanding of the foundations of our institutions of property and ownership, an understanding of why we own things. In the domain of software we can ask whether our purposes are better served through greater or lesser degrees of ownership: legal principles are still sufficiently flexible to make it worthwhile considering what kinds of laws concerning software ownership would be most helpful to the computing community.

A. Contemporary legal mechanisms

The main justification for any laws establishing ownership of software (i.e., proprietary software) is that profit is the incentive for software development and profit can only be realized through ownership and subsequent sale, or licensing, of it. But the nature of software makes its ownership difficult to define. Three different kinds of law have been used to establish ownership and control of software and each has some problems. The kinds of law are copyright law, the law of confidence (trade secrets), and patent law.

1. Copyright

For copyright purposes a computer programme is defined as "a set of statements or instructions used directly or indirectly in a computer in order to bring about a certain result." By referring to instructions used "directly or indirectly" the definition includes both the source programme and the object programme. What the definition does not include is the idea behind the programme, the algorithm. The law of copyright applies to the *expression* of the idea, not to the idea itself.

The main difficulty in the use of copyright law to protect software property rights is in the more general aspects of programmes, their "structure, sequence and organization", and especially in the user interfaces of programmes, their "look and feel". In these aspects the underlying code can be quite different but still give rise to the same look and feel.

2. Trade secrets

Trade secrecy laws generally give a company the right to keep certain kinds of information secret. The laws are aimed at protecting companies from having competitors find out what it is about their products that give them an advantage in the marketplace. The social utility of such laws is that they encourage improvement of products or production techniques by establishing the rights of business to keep secret the method of those improvements. In general, for a company to claim that some information constitutes a trade secret, it must satisfy four requirements:

(1) The information must be novel in some way;
(2) It must represent an economic investment
(3) It must have involved some effort to develop
(4) The company must make an effort to keep it secret.

Software typically satisfies the first three requirements, but the fourth requirement is sometimes more difficult - particularly when the software is sold. With software that is kept "in-house" the standard device of a nondisclosure clause in the contract of employment can be used. For software that is distributed, the software can be licensed rather than sold, where the licence requires the licensee not to reveal the "secret", i.e., not sell or give away copies of the software.

3. Patent

The strongest form of protection for software is patent protection. With a patent on an invention, the owner of the invention has two enormous advantages. First she has the right to the exclusive production, use and sale of the invention, or to license others to do these things. Second she has the right to exercise this exclusive control even if the invention is later reinvented by someone else. Clearly the possibility of obtaining a patent is an incentive to invent useful things that can be sold. But there is a deeper social purpose of patents. The way patent law works, in order to obtain a patent it is necessary for the invention to be sufficiently clearly described that anyone familiar with the technology involved can reproduce it. Moreover this description is made public in the process of patenting the invention. So not only are the individual's rights of possession established, but the existence of the invention and how it works are made public. In this way others are able to learn from and build on earlier inventions. But the original invention remains the exclusive property of the original inventor.

B. The Basis of property law

To try to resolve and clarify questions about possession of software it is worth considering how laws of property are justified in the first place. Traditionally there are two ways in which we can try to justify laws of property. We can try to justify them on the basis of a natural right of ownership, or we can try to justify them on the basis of their consequences.

1. Natural rights

a. The argument for ownership

The justification of ownership based on natural rights appeals to the idea that a person has a natural right to possess what she produces. The labour that she puts into her production is hers to begin with and thus the product of her labour should remain hers. The product would not have existed without her labour, it is composed, at least in part, of her labour. As such it should remain hers, she has a right to own it.

b. Replies

In the case of software this argument seems to miss the point. If the product of a person's labour is a programme, then she still has it even if someone copies it. If I make a pot out of clay from the common, and you take it from me, then I don't have it any more. But if I write a programme and you copy it out of my files I still have it. So why do I object to your taking it in this way? The only objection can be in terms of some advantage I might gain by having exclusive use of it, in particular the financial advantage I gain by selling it. But we can imagine a world where software never enters the commercial realm? We can easily imagine a world where software is published like scientific articles and the writer is rewarded in the same way as scientists are rewarded for their publications. In this world we would be highly motivated to publish our software. It seems that the morality of software ownership depends on the social system in which we live. In other words, software ownership, at least, seems not to be a natural right.

2. Consequences

a. The argument for ownership

The central motivation for maintaining the right to own software is the profit motive, and this is justified on the grounds that innovation will only come about if there is some advantage to be gained. On this basis, the right to own software is not a natural right but a social right that is justified in terms of its beneficial social consequences. The socially desirable consequences are progress and development of software. This progress and development, it is argued, will not take place unless those who make the effort to bring it about can see something in it for themselves. And that, it is claimed, is profit. The only way to guarantee profit for the producers of software is to give them control over the use and distribution of the software. They can then sell or license it for whatever profit they can get. It is argued that this system has the advantage that quality will be maximized through competition in the marketplace. Software of higher quality will naturally attract higher profits and so the sellers of software will strive to improve their software. This is the consequentialist argument for the social right to ownership.

b. Replies

In the early days of computing people developed software without the profit motive. The motive then was interest, curiosity, intellectual challenge, and, of course, need. Those who created useful software were rewarded within the computer community by the respect and appreciation of those who where able to benefit from the use of the software. In science this is still the prevailing way in which good work is rewarded. Publication of scientific work is the hallmark of success, the work is then available to the scientific community to use and build on as it sees fit. It is not hard to imagine a similar kind of reward system being used in the production of software. Of course if software developers were not to take their income from the marketplace, they would require another source of income. Funding for software developers would have to come from another source. In science this comes from government spending on universities and through research councils. And it is not impossible to imagine a similar source of funding for software developers. But this would depend on further government spending and thus on the political climate. If the political climate favours private sector enterprise, then the science model of software development will not work.

C. Proprietary software vs. free software

The institution of proprietary software is not a matter of some kind of ultimate objective right or wrong, but is a matter of consequences within a particular social system. For that reason we cannot

simply decide through reason alone whether it is morally right to freely copy software but, rather, we must consider what this means in our own social context. The fundamental principle of this discussion so far has been that progress in the development of software is a good and desirable end. Our assessment of the consequences of software ownership has been based on this principle. But there is an intrinsic dilemma that seems to arise from this principle. That is that ownership of software both serves as an incentive for progress and serves to inhibit progress.

1. The basic dilemma - incentive vs. progress

In the late 1970s and early 1980s there was considerable concern about the extent of piracy and illegal software copying and the damage this might do to the software industry. The worry was that without the profit from software sales the industry would collapse and software development and progress would come to a halt. But since the 1990s the opposite kind of concern is being expressed - fears that too much ownership and control might interfere with software development. This illustrates the basic dilemma in thinking about software ownership. If too little ownership is allowed then development is unmotivated and if too much ownership is allowed then development is stifled. If too little is owned then there is nothing for the potential developer to sell, there is no profit to motivate development. But if too much is owned then development is stifled for two different reasons. The first reason is that building on previous developments requires licenses and agreements from those who own the software that embodies those previous developments, and this takes time and costs money. The second reason is that to establish ownership of some new development a costly and time consuming search has to be made to establish that that development is not already owned. Either way, if very much of software is owned it costs time and money to make further developments.

2. The alternative to software ownership

In the early days of computing, programmes were collectively owned and publicly available for free. But they were free not just in the sense that they were shared, as opposed to sold, they were free in the sense that programmers could freely change or modify the programmes. This tradition has been preserved through the work of Richard Stallman and the Free Software Foundation (FSF). There are two senses in which free software can be free - free in the sense of free beer, or free in the sense of free speech. For the FSF, free software is a matter of the users' freedom to run, copy, distribute, study, change and improve the software. This includes both kinds of freedom, but it does not preclude the sale of free software. It also implies that the software source code must be made available to enable changes and improvements to be made. For this reason free software is often referred to as open source software.

Stallman defends the vision of free software with various arguments. He argues in general that software should not have owners, that there is no right of ownership for software because the owner does not lose anything if the software is copied. For this reason he argues that making a copy of software cannot be regarded as theft. In reply to the consequentialist argument that software should be proprietary for economic reasons, Stallman argues that most people who copy software would not have bought it anyway so there is really no economic loss. He further argues that proprietary software *reduces* wealth, and does so in two ways: first by confining the use of the software to those few who have actually paid to use it; and second by prohibiting growth and development of new software based on the proprietary software. In contrast the open-source, free software community increases wealth by making software widely available, both for use and for development. In general Stallman sees open-source, free software as a step towards a future utopia in which there is no scarcity and everyone shares equally in the benefits of mass production.

The benefits seen in free, open-source software are many: (1) By developing software in an open and co-operative way progress is improved because there is no needless duplication of effort. (2) Users who want changes in the programme can make them for themselves. (3) Software support is easier to find - the user doesn't need to return to the producer, she can turn to any local software worker who can assess the problem by looking at the source code. (4) If a genuine error is found in the source code that can be reported back to the community and all will benefit. (5) It will benefit schools and education in general - it will encourage people to learn about programming because they can see how things are done with computers and they will be encouraged to develop their own programmes. And last, but not least, (6) the movement makes computing less expensive - society will not be burdened with the legal wrangling about who owns what, software will be less expensive or free, and service will be more easily obtained.

One of the most immediate dangers facing the free software movement is that unprotected free software can be patented by predatory businesses. To protect against this danger the FSF has developed a way of safeguarding the public availability of free software. Instead of simply placing software into the public domain where it runs the risk of proprietary pre-emption, the software is given a legal protection called 'copyleft': "To copyleft a program, we first state that it is copyrighted; then we add distribution terms, which are a legal instrument that gives everyone the rights to use, modify, and redistribute the program's code or any program derived from it but only if the distribution terms are unchanged. Thus, the code and the freedoms become legally inseparable."

Dr. Richard C. Jennings
Professional Practice and Ethics