Understanding Ethical and Social issues related to systems

Ethics refers to the principles of right and wrong that individuals, acting as free moral agents use to make choices to guide their behaviour. Information technology and information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights and obligations. Like other technologies, such as steam engines, electricity, telephone and radio, information technology can be used to achieve social progress, but it can also be used to commit crimes and threaten cherished social values. The development of information technology will produce benefits for many and costs for others. When using information systems, it is essential to ask, what is the ethical and socially responsible course of action?

A model for thinking about ethical, social and political issues

Ethical, social and political issues are closely linked. The ethical dilemma you may face as a manager of an information system typically is reflected in social and political debate. Imagine society as a calm pond on a summer's day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organisations) have developed well-honed rules of behaviour, and these are backed by laws developed in the political sector that prescribe behaviour and promise sanctions for violations. Now toss a rock into the centre of the pond. But imagine instead of a rock the disturbing force is a powerful shock of new information technology and systems hitting a society more or less at rest. What happens? Ripples, of course.

Suddenly individual actors are confronted with new situations not often covered by the old rules. Social institutions cannot respond overnight to these ripples – it may take years to develop etiquette, expectations, social responsibility, politically correct attitudes or approved rules. Political institutions also require time before developing new laws and often require the demonstration of real harm before they act. In the meantime you may have to act. You may be forced to act in a legal "grey area"

We can use this model to illustrate the dynamics that connect ethical, social and political issues. This model is also useful for identifying the main moral dimensions of the information society which cut across the various levels of action – individual, social and political.

Information rights – Privacy and freedom in the Internet age

Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organisations, including the state. Claims to privacy are also involved at the workplace; millions of employees are subject to electronic and other forms of high tech surveillance (Ball, 2001). Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable and effective.

The claim to privacy is protected in the US, Canadian and German constitutions in a variety of different ways, and in other countries through various statutes. In the US

the claim of privacy is protected primarily by the first amendment, guarantees the freedom of speech and association, the fourth amendment protects against unreasonable search and seizure of ones personal documents or home, and the guarantee of due process.

Due process has become a key concept in defining privacy. Due process requires that a set of rules or laws exist that clearly define how information about individuals will be treated, and what appeal mechanisms are available. Perhaps the best statement of due process in record keeping is given by the Fair Information Practices Doctrine developed in the early 70s.

Most American and European privacy law is bases on a regime called Fair Information Practices (FIP) first set forth in a written report in 1973 by a federal government advisory committee (US dept. of health, education and welfare, 1973). **Fair Information Practices (FIP)** is a set of principles governing the collection and use of information about individuals. The five principles are:

1. There should be no personal record systems whose existence is a secret.
2. Individuals have rights of access, inspection, review and amendment to systems that contain information about them.
3. There must be no use of personal information for purposes other than those for which it was gathered without prior consent.
4. Managers of systems are responsible and can be held accountable and liable for the damage done by systems.
5. Governments have the right to intervene in the information relationships among private parties.

FIP principles are based on the notion of a "mutuality of interest" between the record holder and the individual. The individual has an interest in engaging in a transaction and the record keeper – usually a business or government agency – requires information about the individual to support the transaction. Once gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individuals consent.

The European Directive on Data Protection

In Europe, privacy protection is much more stringent than in the US. European countries do not allow businesses to use personally identifiable information without consumer's prior consent. On October 25th 1998, the European Commission's Directive on Data Protection came into effect, broadening privacy protection in the EU nations. The directive requires companies to inform people when they collect information about them and to disclose how it will be stored and used. Customers must provide their informed consent before any company can legally use data about them, and they have the right to access that information, correct it, and request that no further data be collected. **Informed consent** can be defined as consent given with the knowledge of all the facts needed to make a rational decision. EU member nations must translate these principles into their own laws and cannot transfer personal data to countries such as the US that don't have similar privacy protection regulations.

Working with the European Commission, the US dept. of Commerce developed a safe harbour framework for US firms. US businesses would be allowed to use personal

data from EU countries if they develop privacy protection polices that meet EU standards. Enforcement would occur in the US using self-policing, regulation and government enforcement of fair trade statutes.

Internet challenges to Privacy

The Internet introduces technology that poses new challenges to the protection of individual privacy that the original FIP principles have been inadequate in addressing. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing and storing communications that pass through it.

Intellectual Property

Contemporary information systems have severely challenged existing law and social practices that protect private intellectual property. Intellectual property is considered to be intangible property created by individuals or corporations. Information technology has made it difficult to protect intellectual property because computerised information can be so easily copied or distributed on networks. Intellectual property is subject to a variety of protections under 3 different legal traditions: trade secrets, copyright and patent law.

Trade secrets

Any intellectual work product – a formula, device, pattern or compilation of data – used for a business purpose can be classified as a trade secret, provided it is not based on information in the public domain. Protections for trade secrets vary from state to state. In general, trade secret laws grant a monopoly on the ideas behind a work product, but it can be a very tenuous monopoly.

Software that contains novel or unique elements, procedures or compilations can be included as a trade secret. Trade secret law protects the actual ideas in a work product, not only their manifestation. To make this claim, the creator or owner must take care to bind employees and customers with nondisclosure agreements and to prevent the secret from falling into the public domain.

The limitation of trade secret protection is that although virtually all software programs of any complexity contain unique elements of some sort, it is difficult to prevent the ideas in the work from falling into the public domain when the software is widely distributed.

Copyright

Copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose for a period of 28 years. The copyright office is there to register copyrights and enforce copyright law with copyright extended to books, periodicals, lectures, dramas, musical compositions, maps, drawings, artwork of any kind and motion pictures. The intent behind

copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work. Most industrial nations have their own copyright laws, and there are several international conventions and bilateral agreements through which nations coordinate and enforce their laws.

Software programs were first registered in the mid 60s and Computer Software Copyrights Acts were passed in the 80s, clearly providing protection for software program code and for copies of the original sold in commerce, and sets forth the rights of the purchaser to use the software while the creator retains legal title.

Copyright protection is clear-cut: It protects against copying of entire programs or their parts. Damages and relief are readily obtained for infringement. The drawback to copyright protection is that the underlying ideas behind a work are not protected, only their manifestation in a work. A competitor can use your software, understand how it works, and build new software that follows the same concepts without infringing on a copyright.

"Look and feel" copyright infringement lawsuits are precisely about the distinction between an idea and its expression. For instance, in the early 90s Apple Computer sued Microsoft Corporation and Hewlett-Packard Inc. for infringement of the expression of Apple's Mac interface. Among other claims, Apple claimed that the defendants copied the expression of overlapping windows. The defendants counterclaimed that the idea of overlapping windows can only be expressed in a single way and therefore was not protectable under the "merger" doctrine of copyright law. When ideas and their expressions merge the expression cannot be copyrighted. In general, courts appear to be following the reasoning of a 1989 case – *Brown Bag Software vs. Symantec Corp.* – in which the court dissected the elements of software alleged to be infringing. The court found that similar concept, function, general functional features (e.g. drop down menus) and colours are not protectable by copyright law (*Brown Bag* vs. *Symantec Corp.*, 1992).

Patents

A patent grants the owner an exclusive monopoly on the ideas behind an invention for 20 years. The intent behind patent law was to ensure that inventors of new machines, devices or methods receive full financial and other rewards of their labour and yet still make widespread use of the invention possible by providing detailed diagrams for those wishing to use the idea under licence from the patent owner. The granting of a permit is determined by the patent office and relies on court rulings.

The key concepts in patent law are originality, novelty and invention. The patent office did not accept applications for software patents until a Supreme Court decision in 1981 that held that computer programs could be part of a patent able process. Since then hundreds of patents have been granted and thousands await consideration.

The strength of patent protection is that it grants a monopoly on the underlying concepts and ideas of software. The difficulty is passing stringent criteria of nonobviousness (e.g. the work must reflect some special understanding and contribution), originality and novelty as well as years of waiting to receive protection.

Challenges to Intellectual Property Rights

Contemporary information technologies especially software, pose a sever challenge to existing intellectual property regimes and therefore, create significant ethical, social and political issues. Digital media differ from books, periodicals, and other media in terms of ease of replication, ease of transmission, ease of alteration, difficulty in classifying a software work as a program, book or even music, compactness – making theft easy, and difficulties in establishing uniqueness.

The proliferation of electronic networks, including the Internet, ahs made it even more difficult to protect intellectual property. Before widespread use of networks copies of software, books, magazine articles or films had to be stored on physical media such as paper, computer disks or videotapes creating some hurdles to distribution. Using networks, information can be more widely reproduced and distributed.
With the www in particular, one can easily copy and distribute virtually anything to thousands and even millions of people around the world, even if they are using different types of computer systems. Information can be illicitly copied from one place and distributed through other systems and networks even though these parties do not willingly participate in the infringement. For example, the music industry is worried because individuals can illegally copy digitised MP3 music files to Web sites where they can be downloaded by others who do not know that the MP3 files are not licensed for copying or distribution. The Internet was designed to transmit information freely around the world, including copyrighted information. Intellectual property that can be easily copied is unlikely to be copied (Cavados 96, Chabrow 96).

The manner in which information is obtained and presented on the web further challenges intellectual property protections (Okerson, 96). Web pages can be constructed from bits of text, graphics, sound or video that may come from many different sources. Each item may belong to a different entity, creating complicated issues of ownership and compensation. Web sites can also use a capability called **framing** to let one site construct an on screen border around content obtained by linking to another website. The first sites border and logo stay on the screen making the content of the new site appear to be offered by the previous site.

Mechanisms are being developed to sell and distribute books, articles and other intellectual property on the Internet, and some copyright protection is being provided by the DMCA (Digital Millennium Copyright Act) of 1998. The DMCA implements a world intellectual property organisation treaty that makes it illegal to circumvent technology-based protections of copyrighted materials. ISPs (Internet Service Providers) are required to "take down" sites of copyright infringers that they are hosting once they are notified of the problem.

Ethical Issues

Central ethical issue – should I copy for my own use a piece of software or other digital content material protected by trade secret, copyright and/or patent law? Is there continued value in protecting intellectual property when it can be so easily copied and distributed over the Internet?

Social issues

Most experts agree that the current intellectual property laws are breaking down in the information age. The ease with which software and digital content can be copied contributes to making us a society of lawbreakers. These routine thefts threaten significantly to reduce the speed with which new information technologies can and will be introduced, therefore threatening further advances in productivity and social well-being.

Political issues

The main property-related political issue concerns the creation of new property protection measures to protect investments made by creators of new software, digital books and digital information. SIIA (Software and Information Industry Association) representing over 1400 software and information content firms (including Microsoft) was formed on 01/01/99 from the merger of SPA (Software Publishers Association) and IIA (Information Industry Association). It lobbies for new laws and enforcement of existing laws to protect intellectual property around the world. It runs an antipiracy hotline for individuals to report piracy activities and educational programs to help organisations combat software piracy.

Computer Crime and Abuse

Many new technologies in the industrial era have created new opportunities for committing crime. Technologies, including computers, create new valuable items to steal, new ways to steal them and new ways to harm others. **Computer crime** is the commission of illegal acts through the use of a computer or against a computer system. Computers or computer systems can be the object of the crime (destroying a companys computer centre or a companys computer files) as well as the instrumant of a crime (stealing computer lists by illegally gaining access to a computer system using a home computer). Simply accessing a computer system without authorisation, or intent to do harm, even by accident, is now a crime. **Computer abuse** is the commission of acts involving a computer that may not be illegal but are considered unethical.

No one knows the magnitude of the computer crime problem – how many systems are invaded, how many people engage in the practice, or what is the total economic damage, but it is estimated to cost more than $1 billion in the US alone. Many companies are reluctant to report computer crimes because they may involve employees. The most economically damaging kinds of computer crime are introducing viruses, theft of services, disruption of computer systems and theft of telecommunications services. “Hackers” is the pejorative term for persons who use computers in illegal ways. Hacker attacks are on the rise posing new threats to organisations linked to the internet.

Computer viruses have grown exponentially during the past decade. More than 20,000 viruses have been documented, many causing huge losses because of lost data or crippled computers. Although many firms now use antivirus software the proliferation of computer networks will increase the profatibility of infections.

Illustrative computer crimes

1. Michael Whitt Ventimiglia, a former information technology worker at GTE corporation, pled guilty to the charge of unintentionally damaging protected computers on May 15th, 2000, at a Verizon Communications network support centre in Tampa. Ventimiglia used his ability to gain access to GTE's secure computers and began to erase data on the computers, entering a command that prevented anyone from stopping the destruction. Ventimiglia's actions created more than $200,000 in damage (Sullivan, 2001).
2. An 11 member group of hackers, dubbed "The Phonemasters" by the FBI, gained access to telephone networks of companies including BT, AT&T Corp., MCI, Southwestern Bell and Sprint. They were able to access credit reporting databases belonging to Equifax and TRW Inc, as well as databases owned by Nexis/Lexis and Dunn & Bradstreet information services. Members of the ring sold credit reports, criminal reports and other data they pilfered from the databases, causing $1.85 million in losses. The FBI apprehended group members Calvin Cantrell, Corey Lindsley and John Bosanac and they were sentenced to jail terms of 2 – 4 years in prison. Other members remain at large (Simons, 99).
3. Santo Polanco, an 18 year old student at the New York Institute of Technology and 26 year old Eric Bilejhy were charged with a scheme to defraud. Both men allegedly raised at least $16,000 through fradulant sales at eBay, Yahoo and other web sites, offering computers for auction that were never delivered after purchasers paid them (Angwin, 00).

In general, it is employees – insiders – who have inflicted the most injurious computer crimes because they have the knowledge, access, and frequently a job related motive to commit such crimes.

All nations in Europe and the US have an act making it illegal to access a computer system without authorisation. Other existing legislation covering wiretapping, fraud and conspiracy by any means, regardless of technology employed is adequate to cover computer crimes committed thus far.

The internets ease of use and accessibility have created new opportunities for computer crime and abuse. One widespread form of abuse is **spamming** in which organisations or individuals send out thousands and even hundreds of thousands of unsolicited email and electronic messages. This practice has been growing because it only costs a few cents to send thousands of messages advertising ones wares to Internet users.