Praise for *Ethical Computing: From Meta Ethics to Data Ethics*

This excellent work by Prof Wanbil Lee is particularly pertinent in these days of increasing concern about the safety of our data and the ethical use of such data. We have all seen alarming examples of how data can be breached, hacked, stolen and used for nefarious purposes by individuals, corporations or even countries. It can be extremely damaging to individuals affected and to the corporations whose data is breached. It also touches on the very current area of AI and its influence on all our lives for good or ill, alerting readers to the arrival of a new world that AI makes an important contribution to accelerate.

This book sets out ways to create ethical cyber ecosystems in which we should operate and is the result of years for research and delivery of papers on the subject. A bonus is that, as indicated, the first ten chapters may be used as the basis of a course on techno-ethical issues at senior undergraduate and postgraduate levels in Computer Science and Information Systems or a textbook or source book on ethical, legal and social issues

Professor Lee's book covers such a wide range of topics which deal with the ethical use of data and information through to the means of arguing cases against this illegal use of such data and is a timely reminder of our obligations as well as a means of taking legal action against perpetrators of either unethical or illegal activity. It also delves into best practice to avoid making errors which can lead to devastating outcomes and outlines the ethical analytics that include Ethical Matrix and the Hexa-dimension Metric which Prof Lee developed for this purpose.

As a very naive user of technology, I found the contents of this book extremely helpful and yet alarming as I realised how little I know of these activities and yet how careful and vigilant one must be when being asked to provide personal data even in routine, casual situations such as answering phone calls, WhatsApp messages, etc. or obtaining, using or storing data/information belonging to others. As a retired physiotherapist and an almost retired professional fundraiser, I can see application across

many fields and not just computer sciences. It is a book which should be read by the many and not just a few academics in the field of computing. I highly recommend this text to anyone with an interest in best practice in the secure set up and use of data.

Alicia Watson OAM, FFIA, CFRM, What'sOn Consulting,
Sydney, Australia

It would be an understatement to say that the topic of cybersecurity has become mainstream, in part due to the proliferation of stories in the media of personal data leaks by corporations and governments all around the world.

As threat actors who perpetrate an attack are generally unknown or faceless entities, individuals who have lost their data direct their response to the organisations who have been attacked and expect the organisation to take responsibility. A response by the organisation of just hiding behind impersonal legal protections can quickly get out of hand, negatively impacting overnight their reputation built up over many years. So organisations need to ensure that they have an ecosystem to address, understand, communicate, and come up with solutions which protect them in the eyes of their clients whose data has been leaked or at least reduce the fallout to a minimum.

The use of ethics as part of that ecosystem can help to solve these cybersecurity challenges.

Addressing this, "Ethical Computing: From Meta Ethics to Data Ethics" by Professor Wanbil W. Lee is a compilation of papers that offer ethical ways to create cybersecurity problem management ecosystems. The author provides structures and principles based on ethics which an organization or individual could adopt in deciding what actions to take when presented with a cybersecurity problem. After completing the book, readers will be left with not just a lot to consider, but also a confidence that comes from taking action based on ethics likely tied to the reader's own personal moral code.

Pierre Herbst, CISA, Hong Kong, previously Head of Internal
Audit for Asia Pacific of an international bank.

Ethical Computing

From Meta Ethics to Data Ethics

By

Wanbil W. Lee

Ethical Computing: From Meta Ethics to Data Ethics

By Wanbil W. Lee

This book first published 2024

Ethics International Press Ltd, UK

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

Print Book ISBN: 978-1-80441-548-1

eBook ISBN: 978-1-80441-549-8

In memory of my parents.

My mother Maria Chui Yung Louie: "*Remember any favour received a thousand years*".

My father Kit Wing Lee: "*Man lives to seek knowledge*".

Dedicated to my wife Becky H. K. Shiu.

Contents

Preface

This book is an edited collection of my papers published and presented at conferences, seminars, and lectures, in recent decades. It is a record of the thoughts behind my passage to evangelizing *Ethical Computing* and seeking *innovative and ethical ways to nurture and create ecosystems and mitigate cybersecurity problems*.

Of the twenty chapters, the first ten may be adapted for a semester course on techno-ethical issues at senior undergraduate and postgraduate levels in Computer Science and Information Systems or a textbook or sourcebook on ethical, legal, and social issues. Chapter 1 sets the scene. The discussion covers the context (the landscape of the cyberspace where we live and work), the change due to the technologies, the problem associated with the benefits and facilities the technologies bring along, and the demand that includes a solution to the problem and the necessary knowledge and skills for achieving the solution. That demand is the mission of the computer professional, a role that the computer professional is expected to play well.

Chapter 2 states an alternative view or a new definition of Computer Ethics, and defines Ethical Computing. Chapter 3 describes the underpinning ethical principles on which Ethical Computing tools and methods rely for support; Chapter 4, the computer-related laws, especially the regulations of data privacy protection.

Chapters 5, 6, and 7 cover the current major issues of Ethical Computing: data privacy, intellectual property (particularly, copyright), digital divide, anonymity, professionalism, netiquette, and cyberbullying; Chapters 8, 9, and 10, the tools and methods.

Chapter 11 discusses the passage starting from the problem to arriving at a solution, a show of applying the tools and methods to the issues presented in the first ten chapters. Chapters 12 and 13 discuss in general terms an ethical approach to address two common information security management concerns: information security development and review, and data privacy protection, respectively.

Chapters 14, 15, and 16 focus on techno-ethical issues arising in the law practice – lawyering and law-enforcing; Chapters 17, 18, and 19 on Computer Auditing, general IT practice, and information engineering, respectively.

Chapter 20 reiterates the significant impact that AI bias has on emerging technologies and echoes the prediction of the coming of a new world. Techno-chats may go one way or another depending on which way AI bias favours. The pattern of our personal life and business conduct will be reshaped in the new world where the inhabitants will face multidimensional legal and ethical challenges. Shortage of food, water and fuel supply, even that of clean (non-polluted) air, will challenge man's basic survival; redefinition of humans, the meaning of marriage and gender (attributing to the advancement in robotics and genetic engineering research) in a homo-bot community, and the like, pose another challenge. And more.

The power exerted by AI over our physical as well as mental welfare is a challenge as close as our doorstep. So drastic and real a problem that it cannot be ignored; we must not hesitate to seek mitigation. Semi-AI is proposed. By design, it aims to enrich the good, to dilute the bad, and to bar the ugly of AI bias.

Of the noteworthy features, one is the *Hexa-Algorithm* (in Chapter 10), a recently developed method grounded in the Hexa-dimension Metric to provide a measure of the quality of a decision, a policy, or an action, and in the Ethical Matrix (adapted from Agriculture to Computing) to provide a holistic view of the ethical issues involved in a project, an episode, or a problem, to identify the stakeholders, and to give the decision makers a feel of the principles that the individual stakeholder holds.

Another is *Semei-AI* (in Chapters 16 and 20), which is a newly developed notion for "a controlled, bias-minimized AI with the full efficacy of AI subject to regulations empowered by legislation". Similar in substance and different in label, the idea of semi-AI emerges in different contexts as reported in the literature.

All chapters follow the same theme – ethical, legal, and social issues in cyberspace and remedial mitigation of the consequences thereof. Not only Computer Scientists and computing practitioners but also scholars and practitioners in Health Sciences, Accounting and Auditing, Law, and Engineering, and other professionals as well as any end users of information technologies may find this book good for reference or a refresher.

Acknowledgements

I have benefited from encouragement and appreciation of my work and my thoughts on the subject matter of this book from Mandel Chan, Heinz Chiu, Jen Hajigeorgiou, Abraham Lam, Francis Lam, Jyh-An Lee, Ben Li, Simon Rogerson, Jan Travers, CP Wong, Wolfgang Zankl, and others. I am particularly grateful for the editorial advice from Alicia Watson and Pierre Herbst.

Wanbil W. Lee, Hong Kong

Chapter 1
Introduction

- This chapter draws on the materials in my lecture notes for a course presented to undergraduate and postgraduate students spanning over three decades (Lee, 2006-12, 2014-21) and the chapters originally published as "Ethical Computing", "Ethical Computing Continues from Problem to Solution", and "Ethical Computing for Data Protection" in the *Encyclopedia of Information Science & Technology* (Lee, 2015, 2018, 2020).

The Context

Cyberspace in which we observe the techno-changes and the moral, cultural, and political issues arising thereof is a social context or socio-techno-context. Consider the issues involved in proprietary software, for example. We need to take into account the *context* because we must consult the intellectual property (IP) laws and the ethical principles in order to define ownership and property rights, respectively. Corporations and government agencies do so through their internal policies to interpret the law and the ethical principles for the context; individuals do so based on their policies concerning the context.

Cyberspace is different from, and similar to, the real space (the physical world where we live); their common denominator comprises (i) the data we generate and use, (ii) the technologies we develop and apply, and (iii) the social issues thereof. Using software systems and algorithms in cyberspace to drive the data to deliver goods to the people in real space is different from using the implement to produce artifacts in real space. The goods delivered can be beneficial (as intended) or harmful (as intended or unintended) depending on the moral sense of the developer and the user of these systems and algorithms, together with the issues arising thereof create a new context, a socio-techno-context or, simply, social context, and poses legal and ethical issues.

The machine (or technologies, prominently, the Internet) *changes* fundamentally the social, economic, and political aspects of the entire world. For example, how individuals see themselves, and how they think about what it means to be a human being are changed. There are changes in the way they work, the way they communicate, the way they are educated, the way they are entertained.

We must understand the context to understand the changes, especially when we wish to see that good consequences are eventuated and bad consequences are avoided or stopped. We must recognize the influence these issues exert on our understanding of the technology and how to fill the policy vacuum (see Chapter 2). The state of the goods depends in many ways on the quality of the data in dealing with these issues; data plays a pivotal role in getting a correct and credible result; data security and protection pose a new *problem*; solving the problem requires new expertise and constitutes a new *demand*.

The Changes

The techno-changes, alluded to earlier, can bring along good or bad results – good for some people and bad for others, or good for the majority or the minority, and vice versa. These changes may enhance or erode important social values; the Internet may impede or facilitate democracy; the technology may increase or decrease risk; human beings may lose control of their lives as Artificial Intelligence takes over decision making; and more possibilities. Consequential upon these possibilities, human lives are improved in some ways, diminished in others; some values are enhanced while others are eroded; and some problems are solved as others are created. But do these changes make human lives better? And more questions. Let us get some clues out by looking into the changes to the finance and banking operations, and the impacts on employment and work-life, digital divide, and democratic values over the Internet.

Finance and Banking Operations

The computer brings about changes in tools but may not affect changes in aims and purposes. Consider, for example, what the computer has done to

the banking industry. On the one hand, banking has been transformed by the computer:

- Individuals can perform transactions remotely and electronically.
- The meaning of *money* has changed as money no longer means coins and paper notes. Also, it moves from one place to another electronically.

On the other hand, banking has not been changed because the purposes and functions stay as they have always been:

- Individuals want to store and accumulate wealth and move their wealth around in various ways to achieve their purposes.
- Banks and the banking industry facilitate these transactions.

Digital Divide

Digital divide refers to the situation where some people have access to modern information technology while others do not. It means that people who use telephones, computers, and the Internet have opportunities denied to people without access to these devices. This term, and the idea behind it, became popular in the mid-1990s when the World Wide Web grew in popularity. It has two different dimensions: *global divide* and *social divide*. The former refers to the disparity in Internet access between more industrialized and less industrialized nations, and the latter refers to the difference in access between the rich and poor within a particular country.

Unequal access can skew social and economic opportunities; it can give some individuals much more power than others – some people regard this as a serious threat to democracy.

- If access to *education* is unequal, there is inequality of opportunity for jobs and positions of authority with some types of employment and work disappearing while some are created. Those disappeared include typists, telephone operators, and so on. Those created are programmers, computer operators and technicians, computer graphic artists, web-page designers, etc.

- The computer is seen as a powerful resource that affects and enhances the quality of education. Hence, poor schools as well as rich schools should have the same opportunity to access. Otherwise, the better schools will be able to provide an even better quality of education while the poorer schools fall even further behind. The computer is also seen as a means to equal educational opportunities as it makes possible the distribution of the same expertise and materials to all.
- The Internet gives individuals the capacity to receive and send information and to form *associations* with others independent of geographic location. Those who are able to send information can influence both their political representatives and other citizens; those who receive information know more about the issues and know more about their representatives. As political decisions are often shaped by interest groups and the Internet facilitates group formation, those who have access are in a much better position to combine forces and have power.
- There are strong and compelling reasons for freedom of speech on the Internet. But there are equally strong reasons to restrict because of access that children can have. Also, because of the Internet's global scope, individuals in one country can get access to information made available in other countries. This makes it difficult to enforce national policies of limiting access to certain kinds of expression.

Work-life and Employment

Prolonged use of a monitor has become an increasingly pressing issue of health and safety, a major contributor to eHealth and eSafety concerns, symptomatic of eyestrain, fatigue, and blurring and double vision (called Video Operator's Distress Syndrome). Repeated use of the hand causes ailments (called Repetitive Strain Injury).

Workplace surveillance and computer monitoring make the so-called eEmployment concern. Workers feel stressed when they find that they are monitored by the computer including recording information about work habits such as phone calls, emails, and computer files. As such, computer

monitoring is viewed as unfair practice by management, which employees interpret as staff distrust, invasion of personal privacy, disregard of human rights, and destroying morale.

Democratic Values over the Internet

The Internet that enables online voting and election, and allows equal access, privacy, decentralization, and so on, amounts to change (support or disturb) democratic values like fairness, accountability, transparency, protection from online abuse, and respect for privacy and human rights. This means citizens can freely and fairly elect representatives to the government, thus the claim: "The Internet is democratic". This claim draws on the following supportive arguments:

- Argument 1 claims that the Internet is democratic because it provides many-to-many interaction; and facilitates unmediated (or censor-free or unamended) interaction/communication in institutionalized forms of communication. The Internet also allows access to institutionalized information and many more sources of information; and makes possible the formation of new associations independent of geographical location.
- Argument 2 claims that given democracy means power in the hands of the individual, and that information is power, the Internet makes vast quantities of information available to (many) individuals; and allows individuals to be senders or providers of information. Note: (i) Information is power only if it is accurate and relevant, and misinformation is not empowering. (ii) There is no guarantee that the information obtained through the Internet provides accurate or useful knowledge. (iii) The Internet can facilitate the spread of misinformation as well as information. (iv) Therefore, the Internet is democratic because information is power and the Internet gives individuals access to information and allows individuals to be senders or providers of information.
- Argument 3 claims that the Internet is democratic because it gives power to the less powerful, and takes power away from the more powerful.

The Problem

Cyber-abuses such as violations of data confidentiality and intrusion of personal data privacy, wreak havoc ubiquitously and continually, rendering impotent extant countermeasures (be they legal means or physical and logical access control methods). Bias will creep in during designing, implementing, and using the technological systems; privacy will be disturbed during and after the application of these systems; erroneous or distorted results thus produced will bring about disastrous consequences, culminating in ethical, legal, and security concerns. The varied cyberthreats and the enormous resultant damages culminate in a mixture of technical, financial, legal, social, ethical, and ecological challenges. Individuals and organizations are subjected, daily and increasingly, to threats of unpredictable financial losses, tarnished reputations, and legal actions; hence they seek remedies helplessly. This is symptomatic of big spending on data protection, cyber-miscreants getting more ruthless and sophisticated, well organized and better equipped. This is one dimension of the problem.

Risk is commonly taken to be physical damage or financial loss because of an inadequate understanding, and misunderstanding, of risk and security issues as a result of *misinterpretation of risk*. Training our heads and hands, and not cultivating our hearts and souls is the result of the *flawed science/technology curricula*. The consequence of this incomplete understanding of risk and flawed education will lead to undesirable corporate policies and design goals, and a dangerous mindset. Aiming at meeting the bottom-line requirements in physical terms, emphasizing hard, tangible, and technical skills, neglecting the intangible, soft, and social considerations, and achieving short-term, foreseeable, egoistic financial gains rather than long-term, altruistic goals, will result in a doomed solution. This is another dimension of the problem.

Data is the pivot and victim. Deciding the policies of data protection is imperative and requires an understanding of the social context, which in turn requires an understanding of the nature of the human relationships involved, institutional purposes and values, and prevailing norms of behaviour. Social context is intertwined with the ethical issues that arise in

that context. Filling the policy vacuum must take into account the social context and the human interactions that take place for social purposes. These transactions are invariably technologically driven. Hence, our behaviours in cyberspace must be considered in a socio-technological context in order to address the changes brought about by the flourishing technologies, and these changes may be benign and at the same time malignant like the good and evil in the physical world. However, there is no sight of an effective means to mitigate the aftermath despite the big spending and virtually unlimited effort. This is yet another dimension of the problem.

Certainly, the problem and the issues arising from the episode of buying and selling software are complex and multidimensional. Who is responsible for the defective software; who is accountable for faulty banking transactions; who is liable for being discriminative in categorizing customers; who is guilty of tampering with political elections? And more.

There is no simple answer to these questions, and to answer them, we need to be clear about what is meant when we say someone is responsible for something or some action, or a person is accountable for something. Someone is responsible for something or some action means that the person (or a government agency or a legal person such as a corporation) is the appropriate agent to respond to (i.e. to give an account for) an event or incident or situation (in this case, the defective software). A person is accountable for something means that this person is responsible for reporting what happened, going to jail or paying compensation, or bearing guilt and remorse for the situation (in this case, a report of the software sold, damage or loss attributing to the defective software, etc.) Further, we need to clearly understand these terms: responsibility, accountability, liability, contractual relationship, negligence, and the buying/selling relationship, and the ethical implications of these terms.

Responsibility

Briefly, responsibility can have four different uses. First, responsibility is used in a situation where individuals are expected to do one of their social roles or perform one of their social duties by being an employee, a parent,

a citizen, a friend, a professional such as a lawyer, a doctor, an engineer, and so on. This is *role responsibility.*

Second, responsibility is used on an occasion when an individual does something (or fails to do something) that causes an untoward event. That person is responsible for being the cause. In general, the cause can be attributed to persons as well as events. Suppose your laptop is hung up, so the cause may be attributed to you, the user, because you are careless, or to the software because it contains bugs, or to the vendor of the software who sells you the unsafe software, or the programmer who wrote the software and had not debugged the software thoroughly and properly, etc. This is *causal responsibility.*

Third, responsibility is used when someone is involved in doing something wrong or is at fault. You may be considered blameworthy when you fail to observe a long-standing instruction. For example, you use an outdated version and get a lousy result because you haven't checked the version number of the software. But you may not be considered blameworthy when you did check the version number (which was correct) and yet got the wrong result because someone mislabeled the version number. This is *blameworthiness.*

Fourth, responsibility is used in situations where the person involved must pay damages or compensate when certain events occur, according to the law. For example, a trainee under your care got hurt during a training session. You are considered liable because you are supposed to take care of the trainee even though you may not be blameworthy or may not be responsible in the causal sense. This is *liability.*

To illustrate, the different uses of responsibility of software vendors who are supposed to have a duty to be honest about the products they sell are as follows:

i. the vendor is irresponsible with regard to *role responsibility* if he lies about the functions of the package when selling to Customer X;
ii. the vendor is in addition *causally responsible* if Customer X suffers losses as a result of the malfunction, or lack of the required functions, of the software;

iii. the vendor is also *blameworthy* for having been dishonest; and
iv. the vendor is *liable* to refund the price of the software and compensate Customer X for the losses when the package crashes, destroying X's database and disrupting his business.

Accountability/ Liability

There is a diffusion of accountability and responsibility because of the *scale and complexity* of some computer systems, the *"many hands"* involved in developing, distributing, and using them, and how computer systems sometimes mediate human decision-making.

Scale and complexity mean that some systems are so large and complex that no single individual can understand in detail what is going on in the system. Holding an individual accountable for the harm that may result from the use of such a system is extremely difficult or impossible.

Many hands implies that mistakes can be made in each of the parts as well as the system as a whole. The design may be flawed; errors may be introduced in the coding; the documentation may be in error, and so on; and errors at any step can lead to harm when the system is used. The many hands involved make it difficult to identify who is accountable. They also make it more difficult for individuals to see themselves as accountable.

To conclude, strict liability has a utilitarian justification as it keeps the pressure on the developers to thoroughly test the software. Considering the producer liable is justified on the following grounds:

- The producer who offers the product for sale to make a profit must bear the risk of loss or injury as this is an invitation to the public, and implicit in the invitation is an assurance that the product is safe.
- The producer is in a better position than anyone else to anticipate and control the risks.
- The producer can spread the cost of injury to buyers by incorporating it into the cost of the product.

Strict liability gives incentive to the producer to be careful, to minimize risks, and to distribute costs. It is utilitarian as it has a positive effect on the following grounds:

- Liability doesn't necessarily prevent the release of faulty products; it discourages their release.
- It opposes the common moral intuition that individuals shouldn't be held responsible for what they can't foresee or prevent.
- It holds producers responsible whether they were at fault, and it does so in order to give them incentive to make efforts to foresee and prevent bad things from happening.

Also, liability justifies legal responsibility, but not moral responsibility, because moral responsibility usually has a strong element of blameworthiness. The *scale and complexity* and the *many hands* involved in developing the systems make it difficult to identify where to lay the blame or to whom the blame is to be laid. Suppose a group of individuals in a software firm does everything reasonable to prevent the occurrence of dangerous flaws in their software, yet a user is hurt as a result of using the software. Utilitarianism justifies holding the firm legally liable to pay for the harm done, but it does not justify the attribution of moral blameworthiness. The group may not be morally blameworthy. It is possible that no one is morally blameworthy or someone did something wrong and is blameworthy. The situations in information technology seem to have more of the former, that is, no one is morally blameworthy.

Given that selling products is treated differently from the provision of services, to assess who is liable for defective software needs to establish if software is a product or a service.

- If we agree that the product is similar to tangible things, then, since software is intangible, it can't be treated as product.
- The storage devices (tapes, disks, etc.), on which software is stored, are tangible but the software itself (though the valuable part) is not tangible. Therefore, software *per se* cannot be accepted as product.
- At this point, whether software is product or service remains undetermined due to its intangibility. However, the intangibility

of software is not the issue as the product liability law doesn't view products as necessarily tangible. For example, leases, energy, etc., which are intangible, are treated as products. Yet the intangibility of software does not determine whether it is a product or service.

- Then what? It is advisable to forget whether the vendor was honest or manipulative and to put aside the idea that all software must be treated the same way, but to focus on *how things are bought and sold*.

How things are bought and sold prompts the notion of category of software, and raises the question as to whether it is justified to imposing liability on the producer, developer, or supplier, or all of them, of the software of various categories. Software can be categorized as ready-made, custom-made, and mixed.

Ready-made: This category refers to mass-produced and mass-marketed, off-the-shelf software packages. Ready-made software is not supposed to be modified and certain options are available but the user is not expected or allowed to change the codes. [Software of this category is treated as a product.]

Custom-made or Tailor-made: This category of software is designed and made according precisely to what the customer specifies to meet special needs. [It is treated as a service.]

***Mixed*: or off-the-shelf and altered-to-fit**: This means buying the "off-the-shelf" (or ready-made) software and hiring someone to "alter-to-fit" (i.e., modify the software to fit) the special needs and circumstances. [Defects found in the ready-made part are treated under the conditions of a *product;* errors made in the process of modification are treated under the conditions of a *service*.]

Strict liability doesn't make sense for customized (or tailor-made) software because the software in this case is not mass-marketed but is created and designed for a particular customer. The producer may not be able to determine the risks of the software or to distribute the costs of paying damages; the client may know more about the risks because the client knows more about the context in which the software will be used. In this

case, the customized software should not be considered a product. In the case of the mass-marketed software being purchased and modified,

- if the error is found in the canned part of the software, then the consequent damage should be viewed (by the law) as a product;
- if the error is found in the process of modification, then the damages should be viewed as negligence in the provision of a service.

Hence, holding individuals or companies strictly liable can have good effects; threatening to make software developers pay damages when their software is found faulty encourages them to take precautions and make their software reasonably safe and reliable before releasing it. It is now clear that mass-marketed software should be treated as a product and strict liability applies. What about customized software and its production if it is considered a service? This can be held accountable through the law on negligence.

Contractual Relationship

Buying and selling is a central part of a contractual relationship – one party agrees to do certain things, and the other party agrees to do something else in return. This relationship is formalized using a written document that spells out all the conditions of the relationship. Disputes do arise despite the details having been spelled out – often buyers don't know exactly what to specify. Many disputes are ended up in the court appealing to case law that deals with various disputes arising from buying and selling. Look up contract laws for more information, and consult the company's legal counsel if involved in dispute at work or elsewhere.

Negligence

Negligence is failure to do something that a reasonable and prudent person would have done. In common law, individuals who engage in certain activities owe a duty of care; negligence is a failure to fulfill that duty. Negligence is often used to describe blameworthy behaviour of members of professional groups. Software engineer, for example, has a responsibility to design software that doesn't crash under normal conditions of use. The

software engineer may be found negligent if his or her design fails repeatedly because the software engineer has failed to do what any competent designer would have known to do. Negligence is complex and contentious because knowledge and technology are continuously changing. To prosecute computer professionals for negligence is difficult because the standards of the computing field change continuously (Prince, 1980).

In the computer industry, like car safety or heathcare, the experts know how to do things above and beyond the standard, but this knowledge is not put into use because of its cost or risk. Experts are not considered derelict when they opt not to do everything possible to make the software reliable. Trade-offs can be made between reliability or safety and adequacy of treatment and risks, costs and other factors.

Role responsibility is made use for assessing negligence this way:

- If role responsibility is clear, it is easy to determine whether an individual is negligent or not;
- if not clear for various reasons, negligence is much harder to determine.

Categorical Imperative and the buying/selling relationship

The Categorical Imperative tells us never treat a person merely as a means but always as an end. Since the seller is using the buyer as a means to make money, selling is immoral. To counterargue, the seller may be helping the buyer as the seller provides something that the buyer needs or wants. Strictly, the Categorical Imperative does not exactly prohibit us from using others as means to our ends.

- A case of unethical trading: If a seller gets someone to buy something by lying about the product or service, or if the seller tricks someone into buying something the person (the buyer) doesn't really want, then the seller has used the buyer merely as a means to the seller's ends. (That's unethical).