**Handouts of Lecture 11 Professional Practices (IT)**

**Lecture Title: Professional Ethics (Cont.)**

**PRINCIPLE 6: PROFESSION**

Software engineers shall advance the integrity and reputation of the profession consistent with the public interest. In particular, software engineers shall, as appropriate:

6.01 Help develop an organizational environment favorable to acting ethically.

6.02 Promote public knowledge of software engineering.

6.03 Extend software engineering knowledge by appropriate participation in professional organizations, meetings and publications.

6.04 Support, as members of a profession, other software engineers striving to follow this Code.

6.05 Not promote their own interest at the expense of the profession, client or employer.

6.06 Obey all laws governing their work, unless, in exceptional circumstances, such compliance is inconsistent with the public interest.

6.07 Be accurate in stating the characteristics of software on which they work, avoiding not only false claims but also claims that might reasonably be supposed to be speculative, vacuous, deceptive, misleading, or doubtful.

6.08 Take responsibility for detecting, correcting, and reporting errors in software and associated documents on which they work.

6.09 Ensure that clients, employers, and supervisors know of the software engineer’s commitment to this Code of ethics, and the subsequent ramifications of such commitment.

6.10 Avoid associations with businesses and organizations which are in conflict with this code.

6.11 Recognize that violations of this Code are inconsistent with being a professional software engineer.

6.12 Express concerns to the people involved when significant violations of this Code are detected unless this is impossible, counter-productive, or dangerous.

6.13 Report significant violations of this Code to appropriate authorities when it is clear that consultation with people involved in these significant violations is impossible, counter-productive or dangerous.

**PRINCIPLE 7: COLLEAGUES**

Software engineers shall be fair to and supportive of their colleagues. In particular, software engineers shall, as appropriate:

7.01 Encourage colleagues to adhere to this Code.

7.02 Assist colleagues in professional development.

7.03 Credit fully the work of others and refrain from taking undue credit.

7.04 Review the work of others in an objective, candid, and properly documented way.

7.05 Give a fair hearing to the opinions, concerns, or complaints of a colleague.

7.06 Assist colleagues in being fully aware of current standard work practices including policies and procedures for protecting passwords, files and other confidential information, and security measures in general.

7.07 Not unfairly intervene in the career of any colleague; however, concern for the employer, the client or public interest may compel software engineers, in good faith, to question the competence of a colleague.

7.08 In situations outside of their own areas of competence, call upon the opinions of other professionals who have competence in that area.

**PRINCIPLE 8: SELF**

Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession. In particular, software engineers shall continually endeavor to:

8.01 Further their knowledge of developments in the analysis, specification, design, development, maintenance and testing of software and related documents, together with the management of the development process.

8.02 Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.03 Improve their ability to produce accurate, informative, and well-written documentation.

8.04 Improve their understanding of the software and related documents on which they work and of the environment in which they will be used.

8.05 Improve their knowledge of relevant standards and the law governing the software and related documents on which they work.

8.06 Improve their knowledge of this Code, its interpretation, and its application to their work.

8.07 Not give unfair treatment to anyone because of any irrelevant prejudices.

8.08 Not influence others to undertake any action that involves a breach of this Code.

8.09 Recognize that personal violations of this Code are inconsistent with being a professional software engineer.

**Analysis of the code**

The preamble to the code points out that there is no mechanical process for determining the correct actions to take when faced with a moral problem. Even two people with similar philosophies may reach different conclusions when confronted with a moral problem. Two Kantians may agree on the basic facts of a moral problem but disagree on how to characterize the will of the moral agent. Two utilitarians may agree on the benefits and harms resulting from a proposed action but assign different weights to the outcomes, causing them to reach opposite conclusions.

The preamble also warns against taking an overly legalistic view of the code. Simply because an action is not expressly forbidden by the code does not mean it is morally acceptable. Instead, judgment is needed to detect when a moral problem has arisen and to determine the right thing to do in a particular situation. While the code is expressed as a collection of rules, these rules are based on principles grounded in different ethical theories. This is not surprising, considering that the code was drafted by a committee. When we encounter a situation where two rules conflict, the preamble urges us to ask questions that will help us consider the principles underlying the rules.

**Alternative, Discipline-Independent List of Fundamental Principles**

Here is an alternative list of fundamental principles derived using that approach:

1. Be impartial.

The good of the general public is equally important to the good of your organization or company. The good of your profession and your company are equally important to your personal good. It is wrong to promote your agenda at the expense of your firm, and it is wrong to promote the interests of your firm at the expense of society.

(Supports clauses 1.02, 1.03, 1.05, 1.07, 3.03, 3.12, 4.01, and 6.05.)

2. Disclose information that others ought to know.

Do not let others come to harm by concealing information from them. Do not make misleading or deceptive statements. Disclose potential conflicts of interest.

(Supports clauses 1.04, 1.06, 2.06, 2.07, 3.01, 4.05, 4.06, 5.05, 5.06, 6.07, 6.08, 6.09,

6.12, and 6.13.)

3. Respect the rights of others.

Do not infringe on the privacy rights, property rights, or intellectual property rights of others. (Supports clauses 2.02, 2.03, 2.05, and 3.13.)

4. Treat others justly.

Everyone deserves fair wages and appropriate credit for work performed. Do not discriminate against others for attributes unrelated to the job they do. Do not penalize others for following the Code. (Supports clauses 5.06, 5.07, 5.08, 5.09, 5.10, 5.11, 5.12, 7.03, 7.04, 7.05, 7.07, and 8.07.)

5. Take responsibility for your actions and inactions.

As a moral agent, you are responsible for the things you do, both good and bad. You may also be responsible for bad things that you allow to happen through your inaction. (Supports clauses 1.01, 3.04, 3.05, 3.06, 3.07, 3.08, 3.10, 3.11, 3.14, 3.15, 4.02, and 7.08.)

6. Take responsibility for the actions of those you supervise.

Managers are responsible for setting up work assignments and training opportunities to promote quality and reduce risk. They should create effective communication channels with subordinates so that they can monitor the work being done and be aware of any quality or risk issues that arise. (Supports clauses 5.01, 5.02, 5.03, and 5.04.)

7. Maintain your integrity.

Deliver on your commitments and be loyal to your employer, while obeying the law. Do not ask someone else to do something you would not be willing to do yourself. (Supports clauses 2.01, 2.04, 2.08, 2.09, 3.01, 3.02, 3.09, 4.03, 4.04, 6.06, 6.10, 6.11, 8.08, and 8.09.)

8. Continually improve your abilities.

Take advantage of opportunities to improve your software engineering skills and your ability to put the Code to use. (Supports clauses 8.01, 8.02, 8.03, 8.04, 8.05, and 8.06.)

9. Share your knowledge, expertise, and values.

Volunteer your time and skills to worthy causes. Help bring others to your level of knowledge about software engineering and professional ethics. (Supports clauses 1.08, 6.01, 6.02, 6.03, 6.04, 7.01, 7.02, and 7.06.)

**Scenario**

Sam Shaw calls the Department of Computer Science at East Dakota State University seeking advice on how to improve the security of his business’s local area network. A secretary in the department routes Mr. Shaw’s call to Professor Jane Smith, an internationally recognized expert in the field. Professor Smith answers several questions posed by Mr. Shaw regarding network security. When Mr. Shaw asks Professor Smith to recommend a software package to identify security problems, Professor Smith tells him that NetCheks got the personal computer magazine’s top rating. She does not mention that the same magazine gave a “best buy” rating to another product with fewer features but a much lower price. She also fails to mention that NetCheks is a product of a spin-off company started by one of her former students and that she owns 10 percent of the company.

**Analysis**

From our list of nine fundamental principles, three are most relevant here:

. Be impartial.

. Disclose information that others ought to know.

. Share your knowledge, expertise, and values.

Searching the list of clauses identified with these fundamental principles, the following ones seem to fit the case study most closely:

1.06. Be fair and avoid deception in all statements, particularly public ones, concerning software or related documents, methods and tools.

Professor Smith was deceptive when she mentioned the most highly rated software package but not the one rated to be a “best buy.”

1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline.

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

6.02. Promote public knowledge of software engineering.

Professor Smith freely provided Sam Shaw with valuable information about network security.

6.05. Not promote their own interest at the expense of the profession, client or employer.

Professor Smith did not tell Sam Shaw that she had a personal stake in the success of the NetCheks software. She did not tell him about the “best buy” package that may have provided him every feature he needed at a much lower price.

Mr. Shaw was asking Professor Smith for free advice, and she provided it. When she freely shared her knowledge about network security, she was acting in the spirit of clauses 1.08 and 6.02, and doing a good thing. However, Professor Smith appears to have violated the other three clauses, at least to some degree. Most important, she did not reveal her personal interest in NetCheks, which could lead her to be biased. The fact that she did not mention the “best buy” package is evidence that she was neither even handed nor completely forthcoming when she answered Mr. Shaw’s question about software packages. Perhaps Mr. Shaw should have heeded the maxim, “Free advice is worth what you pay for it.” Nevertheless, the ignorance or foolishness of one person does not excuse the bad behavior of another. Professor Smith should have revealed her conflict of interest. At that point Mr. Shaw could have chosen to get another opinion if he so desired.

Scenario

Joe Green, a system administrator for a large corporation, is installing a new software package on the PC used by employee Chuck Dennis. The company has not authorized Joe to read other people’s emails, Web logs, or personal files. However, in the course of installing the software, he accidentally comes across directories containing files with suspicious-looking names. He opens a few of the files and discovers they contain child pornography. Joe believes possessing such images is against federal law. What should he do?

Analysis

Looking over the list of nine fundamental principles, we find these to be most relevant to our scenario:

. Be impartial.

. Respect the rights of others.

. Treat others justly.

. Maintain your integrity.

The list of clauses associated with these four fundamental principles and identify those that are most relevant:

2.03. Use the property of a client or employer only in ways properly authorized, and with the client’s or employer’s knowledge and consent.

Somebody has misused the company’s PC by using it to store images of child pornography. By this principle Joe has an obligation to report what he discovered.

2.09. Promote no interest adverse to their employer or client, unless a higher ethical concern is being compromised; in that case, inform the employer or another appropriate authority of the ethical concern.

While revealing the existence of the child pornography may harm the employee, possessing child pornography is illegal. Applying this principle would lead Joe to disclose what he discovered.

3.13. Be careful to use only accurate data derived by ethical and lawful means, and use it only in ways properly authorized. Joe discovered the child pornography by violating the company’s policy against examining files on personal computers used by employees.

5.10. Provide for due process in hearing charges of violation of an employer’s policy or of this Code. Simply because Chuck had these files on his computer does not necessarily mean he is guilty. Perhaps someone else broke into Chuck’s computer and stored the images there. Our analysis is more complicated because Joe violated company policy to uncover the child pornography on Chuck’s PC. Once he has this knowledge, however, the remaining principles guide Joe to reveal what he has discovered to the relevant authorities within the corporation, even though management may punish Joe for breaking the privacy policy. There is the possibility that Chuck is a victim. Someone else may be trying to frame Chuck or use his computer as a safe stash for their collection of images. Joe should be discreet until a complete investigation is completed and Chuck has had the opportunity to defend himself.

Scenario

The Internet is plagued by a new worm that infects PCs by exploiting a security hole in a popular operating system. Tim Smart creates an antiworm that exploits the same security hole to spread from PC to PC. When Tim’s antiworm gets into a PC, it automatically downloads a software patch that plugs the security hole. In other words, it fixes the PC so that it is no longer vulnerable to attacks via that security hole. Tim releases the antiworm, taking precautions to ensure that it cannot be traced back to him. The antiworm quickly spreads throughout the Internet, consuming large amounts of network bandwidth and entering millions of computers. To system administrators, it looks just like another worm, and they battle its spread the same way they fight all other worms.

**Analysis**

These fundamental principles are most relevant to the antiworm scenario:

* Continually improve your abilities.
* Share your knowledge, expertise, and values.
* Respect the rights of others.
* Take responsibility for your actions and inactions.

Examining the list of clauses associated with each of these fundamental principles reveals those that are most relevant to our case study:

1.01. Accept full responsibility for their own work.

Tim tried to prevent others from discovering that he was the author of the antiworm. He did not accept responsibility for what he had done.

1.08. Be encouraged to volunteer professional skills to good causes and contribute to public education concerning the discipline. The antiworm did something good by patching security holes in PCs. Tim provided the antiworm to the Internet community without charge. However, system administrators spent a lot of time trying to halt the spread of the antiworm, a harmful effect.

2.03. Use the property of a client or employer only in ways properly authorized, and with the client’s or employer’s knowledge and consent. Tim’s “client” is the community of Internet PC owners who happen to use the operating system with the security hole. While his antiworm was designed to benefit them, it entered their systems without their knowledge or consent. The antiworm also consumed a great deal of network bandwidth without the consent of the relevant telecommunications companies.

8.01. Further their knowledge of developments in the analysis, specification, design, development, maintenance, and testing of software and related documents, together with the management of the development process.

8.02. Improve their ability to create safe, reliable, and useful quality software at reasonable cost and within a reasonable time.

8.06. Improve their knowledge of this Code, its interpretations and its application to their work.

Tim followed the letter of the first two of these three clauses when he acquired a copy of the worm, figured out how it worked, and created a reliable antiworm in a short period of time. The experience improved his knowledge and skills. Perhaps he should invest some time improving his ability to interpret and use the Code of Ethics!

**Whistle Blowing**

A whistle-blower is someone who breaks ranks with an organization in order to make an unauthorized disclosure of information about a harmful situation after attempts to report the concerns through authorized organizational channels have been ignored or rebuffed. Sometimes employees become whistle-blowers out of fear that actions taken by their employer may harm the public; other times they have identified fraudulent use of tax dollars.

Consider a person who has known about a dangerous product for years but only becomes a whistle-blower after he has been turned down for a raise or promotion. If the disgruntled employee blows the whistle in order to exact revenge on an organization that has let him down, the primary motivation is to hurt the company, not to help the public. Another example of questionable whistle-blowing is the case of employees who have been involved in a cover-up for some period of time, realize that they are about to be caught, and then cooperate with the authorities to identify other guilty parties in order to avoid punishment. But suppose a person doesn’t have ulterior motives for whistle-blowing and is doing it simply to inform the public of a dangerous situation or a misappropriation of funds. There are three general reactions to altruistic whistle-blowing

**Motives of Whistle-blowers**

People become whistle-blowers for different reasons

Morality of action may depend on motives

Good motive

Desire to help the public

Questionable motives

Retaliation

Avoiding punishment

**Corporate Response to Whistle-blowing**

The typical corporate response to whistle-blowing is to condemn it. Whistle-blowers are disloyal to their companies. Through their actions they generate bad publicity, disrupt the social fabric of an organization, and make it more difficult for everyone to work as part of a team. In other words, their betrayal causes short-term and long-term damage to the company. While it is the responsibility of engineers to point out technical problems, the management of a company is ultimately responsible for the decisions being made, both good and bad. If management makes a mistake, the public has recourse through the legal system to seek damages from the company, and the board of directors or CEO can replace the managers who have used bad judgment. The weakness in this response is its cavalier and overly legalistic attitude toward public harm. If people are hurt or killed, they or their heirs can always sue for damages. Yet surely society is better off if people are not harmed in the first place. A monetary settlement is a poor replacement for a human life.

**Whistle-blowing as Organizational Failure**

A second response to whistle-blowing is to view it as a symptom of an organizational failure that results in harm all around. The company suffers from bad publicity. The careers of accused managers can be ruined. It makes people suspicious of one another, eroding team spirit. Whistle-blowers typically suffer retaliation and become estranged from their coworkers. Labeled as troublemakers, their long-term prospects with the company are dim. Since whistle-blowing is a sign of failure, organizations need to find a way to prevent it from happening in the first place. Some suggest that organizations can eliminate the need for whistle-blowing by creating management structures and communication processes that allow concerns to be raised, discussed, and resolved. This may be easier said than done. Robert Spitzer observes that organizations have shifted away from principle-based decision making to utilitarian decision making. A characteristic of rule-oriented ethical decision making is its absolute nature. According to Kantianism or social contract theory, the end never justifies the means. If an action violates a moral rule, it shouldn’t be done, period. In contrast, a utilitarian process weighs expected benefits and harms. Once an organization begins using utilitarian thinking, the question is no longer “Should we do it?” but “How much of it can we do without harm?” Spitzer writes, “One can see situations in which it would be permissible to use an evil means to achieve a good so long as enough benefit can be actualized.” He suggests that organizations should return to using principle-based ethics in their decision making.

**Whistle-blowing as Moral Duty**

Richard De George believes whistle-blowers should ask themselves five questions:

1. Do you believe the problem may result in “serious and considerable harm to the

public”?

2. Have you told your manager your concerns about the potential harm?

3. Have you tried every possible channel within the organization to resolve the problem?

4. Have you documented evidence that would persuade a neutral outsider that your view is correct?

5. Are you reasonably sure that if you do bring this matter to public attention, something can be done to prevent the anticipated harm?

According to De George, you have a right to whistle-blow if you answer yes to the first three questions; if you answer yes to all five questions, you have a duty to whistle blow.

De George’s five requirements are controversial. Some would say whistle-blowing is justified even when fewer requirements are met. For example, what if the potential whistle-blower knows about a problem that could result in death or injury to millions of people, such as a meltdown inside a nuclear power plant? The whistle-blower has communicated his concerns to his manager, but there is not time to lobby every potential decision maker in the company. He is reasonably sure that if he contacted a television station, something could be done to prevent the meltdown. At the very least, the media could alert people so that they could get out of harm’s way. Shouldn’t that person be obliged to whistle-blow, even though the answer to the third question is no?

To others, insisting that the whistle-blower have convincing documentation is too strict a condition to be met in order for whistle-blowing to be a moral imperative. After all, once the whistle-blower has revealed the wrong to another organization, that organization may be in a better position to gather supporting evidence than the whistleblower. Along the same line, some argue that whistle-blowing should be considered an obligation even when only the first three requirements are met. They hold that people should be willing to sacrifice their good and the good of their families for the greater good of society. Others believe De George goes too far when he gives conditions under which people are morally required to whistle-blow. These commentators suggest that a person’s obligation to whistle-blow must be weighed against that person’s other obligations, such as the duty to take care of one’s family.

Moral responsibility is different from other kinds of responsibility. First of all, moral responsibility must be borne by people. While the Fourteenth Amendment to the Constitution may make a corporation a person in the legal sense of the word, a corporation is not a moral agent. We cannot assign moral responsibility to a corporation or any other organization. Second, moral responsibility is different from role responsibility, causal responsibility, and legal responsibility in that it is not exclusive. Role responsibility is responsibility borne because of a person’s assigned duties. A company may hire a bookkeeper to send out invoices and pay the bills. It is the bookkeeper’s responsibility to get the bills paid on time. Causal responsibility is responsibility assigned to people because they did something (or failed to do something) that caused something to happen. “Joe is responsible for the network being down, because he released the virus that caused the computers to crash.” Legal responsibility is responsibility assigned by law. Homeowners are responsible for the medical bills of a postal carrier who slips and falls on their driveway. Role responsibility, causal responsibility, and legal responsibility can be exclusive. For example, if one person is responsible for paying the bills, the other employees are not. Moral responsibility is not exclusive. For example, if an infant is brought into a home, both the mother and the father are responsible for the baby’s well-being.

***Reference:***

***Lecture topic: Professional Ethics slides***

***Ethics for the Information Age by Michael J. Quinn***