Teaching a Course on "Social Implications of Computing" in Undergraduate Curriculum

Narayan Debnath, Eugene Lundak, Paul Schumacher
Computer Science Department
Winona State University
Winona, MN 55987
e-mail: {NDebnath, ELundak,PSchumacher}@winona.edu

Abstract

Based on the recommendations of IEEE and ACM, the Computer Science Department at Winona State University has been offering a course on Social Implications of Computing as part of the undergraduate curriculum. The course is required for all majors in computer science and applied computer science. The course provides an overview of the societal and ethical issues surrounding computer technology and involves students in discussions about the social implications of this technology. Primary topics include professional ethics, privacy, intellectual property, computer and network security, computer reliability, work and wealth, and the societal impacts of computing, networking, and information storage and retrieval. The course involves extensive reading, writing, and discussion. This paper will discuss the topics and techniques used in teaching this course as well as students learning outcomes expected from the course for evaluating its success in the curriculum. This paper may help other universities improve/develop a computer science curriculum by including such topics and/or by offering a complete course focusing on these topics in the future information age.

1. Introduction

The course entitled Social Implications of Computing (CS 310) at Winona State University (WSU) provides an overview of the societal and ethical issues surrounding computer technology and involves students in discussions about the social implications of this technology. Discussions include topics such as professional ethics, privacy, intellectual property, computer and network security, computer reliability, work and wealth, and the societal impacts of computing, networking, and information storage and retrieval.

This course requires extensive writing and satisfies WSU University Studies Program Writing Flag requirements. It involves writing documents/reports, followed by revising and/or editing documents/reports, on the topics including growth of computer and information technology, introduction to ethics, networking, intellectual property, privacy, computer and network security, computer reliability, professional ethics, work and wealth, and plagiarism. In addition, the course requires writing a major research paper, following the standard format, addressing the advances, social implications and ethical issues in software engineering, networking or databases.

As a Writing Communication Flag course, CS 310 requires a significant amount of written work. Writing assignments comprise a significant portion of the course grade and students have opportunities to obtain student and faculty critiques of their writing.

The paper is organized as follows. Section 2 presents the contribution of the course to writing flag requirements. Section 3 provides information about course objectives, expectations and student learning outcomes. Section 4 discusses the general and specific course outcomes. Section 5 describes a brief description of the topics covered in the course followed by a list of the text and additional reference.

2. Contribution of the Course to Writing Flag Requirements

(a) Learning activities to practice the processes and procedures for creating and completing successful writing in the field

The course requires extensive technical writing throughout the semester on various topics of ethics for the information age and social implications. The significant part of the students' grade is based on the written reports produced during the semester and final major research paper submitted at the end of the semester. Students write summary/report using a specified format on topics including ethical theories, intellectual properties, copyrights, privacy, computer and network security etc. using the procedures and processes they learned earlier in their computer science courses as well as in the current course. Students incorporate the practices and procedures into their summary, reports and research document. At the end of the semester, students are required to submit a major and complete research paper on progress, ethical issues and social implications on a specified topic to demonstrate technical writing skill in the field. Documentations and refinements are ongoing activities and must be applied continuously throughout the preparation and writing of the papers and reports. Writing documents on any computer science topic is an iterative process and goes through continual refinements/improvements by using the feedback/comments from the instructor and other students throughout the semester.

(b) Learning activities to understand the main features and uses of writing in the field

The theory and lectures learned throughout the first year computer science course sequences on algorithms and problem solving as well as a basic English course (which are the prerequisites for this course) along with the materials of the current course on social implications in computing are put into practice. These help students to understand and express the concepts required to appropriately and accurately express the contents for the reports and the major research paper.

(c) Learning activities to adapt the writing to the general expectations of readers in the field

Students must learn to articulate, through writing, the language/notations specific to information and software technology. Students are in a position of writing and reporting the technological progress and challenges, social implications, and ethical theories and practices in a meaningful way to the readers in the field. The concepts of computer and professional ethics, privacy, computer and network security, intellectual property, human-computer interactions are learned through research and report writing, and the continuous feedback on the report from the instructor ensures the expectations of readers in the field. The course provides an opportunity to develop writing skills specific to computer science and information science disciplines throughout all assignments in this course as well as written assignments that are developed and graded throughout the semester.

(d) Learning activities to make use of the technologies commonly used for research and writing in the field

The current course deals with the theory, concepts, applications and implications of software and information technology by studying/analyzing the existing technology. Therefore, it is imperative that students directly utilize the current technology and existing software tools in writing the research documents and reports throughout the semester in the course. This activity is very useful in research and writing reports/documents in this field.

(e) Learning activities to learn the convention of evidence, format, usage, and documentation in the field.

Students are required to learn and adapt a standard format of writing a technical report in the field. This includes title page, abstract, introduction, objectives, research contributions, interpretation of results, comparisons with theory, conclusions, recommendations, possible future research, references, and appendices. As students learn the social and ethical implications of computing and information age through report and documentation, they also learn to articulate the skills of application of theory and scientific principles that support the current progress and developments in the field of computing and information technology. Written assignments are intended to prepare the students for the critical thinking and documentation skills necessary for employment and success in the field.

Students get continuous feedback throughout the semester on their reports and writings from the instructor. The final reports/documents submitted for the course incorporate all comments, suggestions and feedback/refinements from the instructor. The technical writing standards, style and format followed in the course are consistent with the format and style used in preparing a technical paper for computer science and/or information technology conferences.

3. Course Objectives, Expectations and Student Learning Outcomes

(a) **Catalysts for Change:** Students are expected to learn the milestones in Computing, milestones in Networking, milestones in information storage and retrieval, and information technology issues.

(b) **Introduction to Ethics:** Students are expected to learn the subjective relativism, cultural relativism, divine command theory, Kantianism, act utilitarianism, rule utilitarianism, social contract theory, comparing ethical theories, and morality of breaking the law.

(c) **Networking:** Students are expected to learn about Email and Spam, fighting spam, World Wide Web, censorship, freedom of expression, children and the web, breaking trust on the internet, and internet addiction,

(d) **Intellectual Property:** Students are expected to learn the intellectual property rights, protecting intellectual property, fair use, new restriction on use, peer-to-peer networks, protections for software, open-source software, and legitimacy of intellectual property protection for software.

(e) **Privacy:** Students are expected to learn the perspectives on privacy, disclosing information, public information, US legislation, public records, covert government surveillance, US legislation authorizing wiretapping, data mining, identity theft, and encryption.

(f) **Computer and Network Security:** Students are expected to learn the viruses, worms and Trojan horses, phreaks and hackers, denial-of-service attacks, and online voting.

(g) **Computer Reliability:** Students are expected to learn the Data-Entry or Data-Retrieval errors, software and billing errors, notable software system failures, Therac-25, computer simulations, software engineering, and software warranties.

(h) **Professional Ethics:** Students are expected to learn about computer experts and professionals, software engineering code of ethics, analysis of the code, and whistle blowing.

(i) **Work and Wealth:** Students are expected to learn the Automation and unemployment, workplace changes, globalization, the digital divide, the winner-take-all society, and access to public colleges.

(j) **Plagiarism:** Students are expected to learn the consequences of plagiarism, types of plagiarism, guidelines for citing sources, avoidance of plagiarism, and misuse of sources and information.

Students are required to write a paper describing the concepts learned on these topics and take a quiz demonstrating a clear understanding. Students are also required to present these topics to encourage in-class discussions and active participations for better understanding and enhanced learning. In addition, students will be required to work on a major research project and write a technical paper describing the technological advances, social implications and ethical issues in one of the specified topics within computer science. The paper is evaluated based on the quality, significance, demonstrated ability in research, and writing skills.

4. General and Specific Course Outcomes

The use of computer technology by students, at this time, is a significant aspect of their lives, and this use will only continue to increase in their lifetime. This course deals with the computer technology and its social implications, so that they can understand and use it more effectively. To understand the societal implications of computer and information technology, it is necessary to expose students to some of the basic scientific foundations of computer technology. From the technical perspective and understanding, the students then study the social, ethical, historical, and political implications of the technology.

(a) understand the scientific foundation of the topic

Students will learn the milestones in Computing, milestones in Networking, milestones in information storage and retrieval, and information technology issues. In addition, students will learn about Email and Spam, fighting spam, World Wide Web, censorship, freedom of expression, children and the web, breaking trust on the internet, and internet addiction.

(b) understand the social, ethical, historical, and/or political implications

The title of this course is *Social Implications in Computing* and the topics it covers directly addresses all of these issues in depth. The course is specifically designed and structured in a way to help enhance students understanding and learning on social, ethical, historical, and/or political implications.

Students will examine the tremendous growth in computer and information technology since the beginning and the impact this growth has had on people, law, and ethics. Political and legal implications become clear when they see how technology has outpaced the legal and political arenas. Students will learn current laws pertaining to copyright, privacy, and accessibility.

In particular, students will focus on introduction to ethical theory and learn the subjective relativism, cultural relativism, divine command theory, Kantianism, act utilitarianism, rule utilitarianism, social contract theory, comparing ethical theories, and morality of breaking the law. Students will learn professional ethics with emphasis on the computer experts and professionals, software engineering code of ethics, analysis of the code, and whistle blowing. The students will also learn the intellectual property rights, protecting intellectual property, fair use, new restriction on use, peer-to-peer networks, protections for software, open-source software, and legitimacy of intellectual property protection for software.

(c) understand and articulate the need to integrate issues of science with social policy

Students will learn about historical and current cases of the abuse of technology. Students will take what they have learned about issues and policies to analyze and evaluate various scenarios.

The students will learn the perspectives on privacy, disclosing information, public information, US legislation, public records, covert government surveillance, US legislation authorizing wiretapping, data mining, identity theft, and encryption. Moreover, students will discuss the automation and unemployment, workplace changes, globalization, the digital divide, the winner-take-all society, and access to public colleges. Students will understand and analyze the consequences of plagiarism, types of plagiarism, guidelines for citing sources, avoidance of plagiarism, and misuse of sources and information.

(d) evaluate the various policy options relevant to the social dilemmas posed by the science

Students will present and discuss several social dilemmas presented in class. These include such things as privacy, digital copyright issues, data mining, and material appropriate/inappropriate for the web, misuse of information, and possible abuse of computer, software and information technologies.

(e) **articulate, choose among, and defend various policy and/or scientific options to cope with the challenges created**

To allow the students the opportunity to discuss and defend policies and scientific options, under each topic or theory presented in the class, several scenarios will be prepared on various topics including ethical theory and analysis, networking, intellectual property, privacy, and professional ethics for extensive discussions and evaluations. These discussions will allow for points of view to be presented and decided on in class. These discussions and presentations will allow students articulate and defend various policy and/or scientific options and to cope with the challenges created.

5. A Brief Descriptions of the Chapters and Topics

The course uses the lecture notes [2] for an introduction on progress and challenges in computer and information technology. This course uses the primarily text book [1] for presentation and discussions of the topics discussed in all the chapters and topics included in the text..

Chapter 1 [1] deals with the history of the different areas of computing including computing, networking, and information storage and retrieval. Some of the earliest computers was made between 1939 and 1941 and was called the Atanasoff-Berry Computer. It was built with vacuum tubes and was not programmable. In 1946 the ENIAC was made, it was a powerful computer for its time and was 2,400 times faster than a person with a desk calculator. The first commercial computer was the UNIVAC and the first programmable, electronic computer was the ENIAC. The ENIAC was built in 1946 to calculate ballistic tables for the United States Military. The ENIAC calculated tables in 30 seconds, the same calculation by hand took over 20 hours. In other words, the ENIAC was 2,400 times faster than a person with a calculator. The ENIAC also had many features of the modern computer. All of the internal components of the ENIAC were electronic, and the ENIAC itself was programmable with wires and switches. Although it was programmable, the programming was tedious and could take days. The Transistor was an important invention that greatly contributed to the advancements of computing. The invention was announced in 1948 by Bell Labs which was a substitute for the vacuum tub. Soon after, the integrated circuit was created in 1957, which allows for circuits and wires to be compacted into a small disk like object. The microprocessor first developed around 1968 contained 2,300 transistors which had the same computing power of the ENIAC in a 1/8” x 1/6” chip. This then led to the personal computer as it was much cheaper to produce and decreased the overall size of the computer. Information storage has become an important part of the computing society as computing data and information is not nearly as efficient if you are required to input the data every time. The codex was an early age written storage item and were made out of sheepskin or calfskin. Newspapers became an important medium in history. Graphical user Interface and hypertext has become an important part in information transmission and viewing. Search engines can provide unlimited information for those who seek it very conveniently.

Chapter 2 [1] gives an introduction to ethics, the concept of rational examination of people’s moral beliefs and behavior, along with the idea of morality, which are the guidelines that indicate the correct action within various circumstances. The chapter goes over many different ethical theories which people use, logical or not, to guide moral decision making. The first category of ethical theory is the relativistic theories, which are based on the thought that morality is invented by people. This implies that there is no universal good or bad. The theories covered by this chapter under this umbrella include subjective relativism in which morality is personally created, and cultural relativism which states that it is society which determines the morality. The issue with relativistic theories is that there is no baseline to determine whether a set of moral guidelines is better than another set. Because of the extreme difficulty of comparison under relativistic theory, these are not used by this book. The second set of theories posed by the text is the objectivist theories. These theories are based on the thought that morality is not a human creation but a creation outside of our minds. Objectivist theories pose that there is a universal morality which is to be followed and these principles of universal morality hold true for all people in all walks of life. The first theory touched on by the text in this section is divine command theory. This theory states that God has provided moral guidelines in order to better improve our being, and must be followed as they are the will of God. The issue comes with the theory in it is to be followed not because the rules are derived from facts we know to be true, but the word of God. The first of the four theories that the book holds useful is Kantianism. Kant was a philosopher who held that duty was the most important motive for morality. Kantianism follows two imperatives which all moral rules must follow, which are: Follow only rules which can be followed as universal laws, and treat people as ends themselves, not means to an end. Kantianism is a non-consequentialist theory. This means that it is not concerned with the consequences of an action, but the will behind it. The next theories talked about are the pair of Act and Rule Utilitarianism. According to this theory, the right or wrongness of an action lays solely on the consequences of an action, the opposite of Kantianism. The difference in the two theories lies in the name. Act Utilitarianism holds that an action is good if it has good results. Rule Utilitarianism holds that an action is good if everybody follows it and it then leads to good results. The final theory discussed is Social Contract theory. This is the theory that morally is the set of governing the treatment of other people that rational people will agree to follow assuming all other people follow these rules. These four theories all have respective strengths and weaknesses, and all have problems which are much easier for a theory to solve than another theory. These four theories form the basis on which the rest of this text is built upon, analyzing different technological situations and complications to deal with.

Chapter 3 [1] covered many important topics involving networking. A network is created when two or more computers are linked together using cables, routers, and hubs. Advances in networking have brought the world closer together than ever. It allows us to use our computers to communicate with others through email, chat, video conferencing, share storage space, exchange files, connect to the World Wide Web and much more. The Internet is a network which contains millions of computers and when linked with the World Wide Web, allows us access to millions of articles of information, shop online, blog, promote businesses, and communicate with anyone in the world who is also connected. Email is the primary use of the Internet which allows people to send messages to one another all across the world. Spam has been a negative result of email, which people send out unsolicited messages to advertise a product or company. In using all analysis' we have, we can conclude that Spam is an immoral act. Spam can be very annoying and frustrating, so people have come up with ways to combat it. Black-listing is a technique used to block senders of Spam from reaching our virtual mailboxes. The CAN SPAM act was put in order in 2003, requiring senders to include their name, allowing recipients to opt out of the messages, and contain the senders' postal address.

Spim is a relatively new term which is the sending of unsolicited messages through instant messaging services. The World Wide Web is an Internet browser which gives us access to the thousands of online websites. There are three main attributes which the World Wide Web contains. First it is decentralized, meaning someone can freely add information without it being checked, second is that every web page has a unique address, and third it is used on the Internet. Pornography has become a large part of the Internet and is viewed in different ways. People who oppose it say that it reduces dignity of human life, offends people, and makes rape more acceptable. Censorship is the act to access to material considered harmful and is usually enforced by the government. Direct censorship is when a government in some way controls aspects of the media and have the final say in what is allowed. Self-censorship is when a group decides not to release content; sometimes to avoid persecution or to keep on good terms with government officials. We in the United States were given the freedom of expression with the United States Constitution but must realize it is not an absolute right. We are not allowed to use slander, misrepresentation, reckless lies, false advertising and other such harmful uses of expression. Web filters can be put in a system to keep unsafe or harmful web pages from being viewed; libraries often use these filters to protect children. The ethical issues with such filters is that although it keeps out pornography and the like, it may also block non pornography web sites and blocks people's right to freedom of expression. The internet has become a gold mine for criminals. Identity theft is a problem increased by the Internet; criminals often send out fake emails and create fake web pages in order to gain peoples secret information.

Chapter 4 [1] discusses intellectual property rights and described what intellectual property rights are and the unique product of the human intellect that has commercial value. This basically means that something that one can sell but isn't tangible is intellectual property. Take music for example the song is written on a sheet of paper, you may own that sheet of paper but the song itself still belongs to the original creator. It is important to distinguish the difference between physical property and intellectual property, just because someone owns the intellectual property doesn't mean they own the physical property. Another major issue is protecting your property. With new technology it becomes easier to steal each other's property by copying a song to a CD. One of the things companies do to make their property easier to prosecute with is trademarks. A trademark or trade mark is a distinctive sign or indicator used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. Another concept is called the patent. A patent is a set of exclusive rights granted by a state to an inventor or their assignee for a limited period of time in exchange for a public disclosure of an invention.

Chapter 5 [1] focuses on the impact that the introduction of information technology has had on the privacy of individuals. When defining privacy, it may be seen as a scale balancing an individual's desires and the desires of society. The individual wishes to keep society out of his or her own business, while society has the responsibility to decide what should be public and what should be private. There is no natural right to privacy, but privacy is a prudential right. In society, people choose to give each other privacy for the good of each other. As people use technology to go about their daily lives, they tend to share a considerable amount of information about themselves, which is kept in databases. This information can be classified as public information, which is information that an organization has received from clients, which it can share with other organizations, as personal information, which is information that a person has prevented from becoming public, and public records, which contain information that has been reported to government agencies. There exist a variety of ways for information to become public. These include body scanners, digital video recorders, the enhanced 911 service, implanted chips, and spyware. With all of the different methods that are available to make personal information public, there comes a need for people to be conscious about where they share their personal information and to whom they share it with. Congress has acted in a variety of ways, through the passing of laws, to protect privacy. For example, the Fair Credit Reporting Act helped ensure the accuracy and privacy of information that was used by credit bureaus and other consumer reporting agencies, and the Children's online Privacy Protection Act made sure that there was not too much information about children out on the Internet. Public records that are kept by the Census Bureau, the Internal Revenue Service, and the FBI contain a considerable amount of information about the public. The Code of Fair Information Practices was the response to concerns about these federal agencies abusing their records. The Privacy Act of 1974 is meant to protect the privacy of U.S. citizens, but it contains so many loopholes that many feel that it hasn't done much to protect privacy. Covert surveillance has been used by various law enforcement organizations and the National Security Agency to collect data. Telegraph and telephone conversations have been eavesdropped on by these agencies, which is a violation of federal law. The Fourth Amendment to the Constitution ruled that not having a court order before performing electronic eavesdropping was a violation of federal law. Data mining allows patterns and relationships to be found through searching through databases of information. It is a method of creation new information through the combination of items in databases. It makes possible the creation of profiles of people by piecing together bits of information that are left about them. It is used by companies to make advertisements that pertain closer to the interests of their customers. Government agencies use data mining to track down unlawful citizens. Identity theft involves misusing another person's identification in order to act as the owner of the stolen identity for monetary gain or access to information. Identity thieves use computerized databases to gain access to the personal records of thousands of individuals. Encryption, which helps keep messages secure by changing them to hide their meaning, is used to keep conversations private. Use of powerful cryptography systems used to be exclusive to governments and businesses, but public-key cryptography systems have allowed others to use cryptography.

Chapter 6 [1] presents Computer and Network Security and discusses various security concerns that can happen to modern day computers. People these days use the internet, the world's largest network, for everything from email to shopping to research for PowerPoint presentations. All this time connected leaves us open to security breaches. These security breaches may come in the form of viruses, worms, or Trojan horses. They may also come from hackers, phone phreaks, or denial-of-service attacks. Online voting is being implemented but could be subject to these breaches. A virus is a computer program hidden inside another program (called the host) that can copy itself and infect a computer. When a user runs the host program the virus runs first, finding another executable program and infecting it. Then the host program is allowed to run. With a good virus, the user never realizes enough time has passed for a virus to run. Since programs are contained on all types of media, viruses can therefore be spread through all those types. There are some viruses that are relatively harmless that do little other than replicate, eating up small amounts of disk space and chewing through a little bit of memory. On the other hand there are viruses that are extremely dangerous and can destroy a person's files and compromise their computer. A worm is a self-replicating computer program that uses a network to send copies of itself to other computers and it does so without any user intervention. There are several well known, famous, and particularly devastating worms. The first worm was the WANK worm. The WANK worm stood for: Worms Against Nuclear Killers. The WANK worm was a classic example of cyber-terrorism. Cyber-terrorism is a politically motivated disruption attack against information systems for the primary purpose of creating alarm and panic. A Trojan horse is a non-self-replicating malware that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system. A Trojan horse performs both the expected task and the malicious task when it is opened. A Remote Access Trojan is a Trojan horse that gives the programmer the ability to get into the computer of prey. Bots are software applications that run automated tasks over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone. Authorization is the idea of specifying access rights to resources, which is related to information security. Authentication is the act of establishing or confirming someone's identity as authentic. Hacking originally expressed admiration for the work of a skilled software developer but has come to refer to someone that cracks into other computers by society. Two ways to get login names and passwords are dumpster diving and social engineering. Phreaking refers to people who study, experiment with, and/or explore telecommunication systems, like equipment and systems connected to public telephone networks. Phreaks typically manage to get free long distance by breaking long distance codes. Phreaks are also responsible for several pranks and attacks over the years. There are several laws regulating computer usage. A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. It isn't designed to steal information, but to disrupt a computer server's ability to respond to its clients. With a DoS attack, a single person can bring massive harm to a large entity in what is called an asymmetric attack. A DDoS is essentially a denial of service attack that is being sent out from thousands of different computers that have been taken over by the bots. SATAN is a security tool that has been developed for system administrators so that they can try and keep their systems as secure as possible.

Chapter 7 [1] deals with Computer Reliability and why the computers may have fault when it is executing, and how these fault will affect the whole system and how to prevent them. There are two different ways may cause the fault relating to data problems: Data-Entry and Data-Retrieval. These faults are because of when people using computers, they may enter wrong data or incorrectly interpret the data. The book lists three examples about Data-Entry and Data-Retrieval fault: disfranchised voters, false arrests and accuracy of NCIC records. Even if people can enter the data correctly, errors still may happen while the computer programs manipulating the data. These errors may lead to a software and billing errors. These errors can lead to system malfunctions, and system failures. As every computer needs a program to execute, a notable software system failure may cause very bad result. Most embedded systems are real-time systems: computers that process data from sensors as events occur. There are examples that illustrate how software may cause failure. The examples of Patriot Missile, Ariane5, and AT&T Long-Distance Network are all good examples of notable software system failure. The field of software engineering grew out of a growing awareness of a “software crisis”. Computers now can execute much larger programs than their predecessors. Programmers responded by designing powerful new operating systems and applications. Unfortunately, their programming efforts were plagued by problems. Usually there are three steps for a programmer to make a program. First is specification. The programmer will decide the purpose for the program based on the user’s request. Then, make a high-level, abstract view of the program, and add details. In the last, they will validate the program. Today, software quality is improved and much more reliable than before. As it is nearly impossible for a program to be perfect, what kind of warranty should a consumer expect to get from software company becomes a topic. Consumer software is often called shrink-wrap software.

Chapter 8 [1] presents Professional ethics. “Professional Ethics” contains discussion on the following main topics: are computer expert’s professionals, the software engineering code of ethics, an analysis of the code, case studies and some examples of whistle blowing. The Software Engineering Code of Ethics and Professional Practice are intended as a standard for teaching and practicing software engineering. It documents the ethical and professional obligations of software engineers. The code is intended as a guide for members of the software engineering field (engineers, educators, managers, supervisors and policy makers), and should be used as a guide post when making decisions or resolving conflicts. This includes the public, the designer, the customer, as well as the company.   The code ethics is based on several ethics models as well as the concept of virtue ethics which was also introduced in this chapter. Virtues, like kindness, selflessness, or charity have value that is dependent on the person. For some, kindness may be the most important virtue while to others charity may be the primary virtue. Although the software code does have an intended order (public first and finishing with the designer last) it is open ended and not “complete” so we are allowed to inject our own virtue ethics into it. The code is made up of seven principles. Principle 1 pertains to the public. That is how what we do affects the public. Software engineers must take full responsibility for their own work and must to the best of their ability make know to the public, through proper channels of course, any grave danger which may be an outcome of their design. Principle 2 concerns the client and the employer. Software engineers must act in a manner that is in the best interest of their employer. This includes utilizing the resources of their employers in an ethic manner, like not surfing the internet, or moonlighting while at work, or promoting interests adverse to the employer or client. Principle 3 is about the product. We must strive for the highest quality of software possible by following professional standards and fully understanding the specifications for which the software must work. Principle 4 is about judgment. Software engineers must maintain integrity and independence in the judgment. That is all decisions must be balanced by the need to support human values. Conflicts of interests must be declared up front so that there are reasonable avenues of escape. And deceptive financial practices must always be avoided. Principle 5, management, relates to the software manager and leaders. It requires that they promote an ethic approach to the management of software development and maintenance. For instance making sure software engineers are aware of all standards for which they may be accountable too. Principle 6 concerns the profession itself. Software engineers should advance the reputation of the profession and be consistent with the public interest. This principle includes helping to develop and environment favorable to acting ethically and supporting other members who strive to follow this code. This includes avoiding those organizations that are in conflict of the code. The seventh principle is about colleagues. Software engineers shall be fair to and supportive of their colleagues. Similar to the sixth principle, software engineers must encourage others to adhere to the code. They must help others in their professional development and credit fully work of others and not take undue credit. They must also give fair hearing to the opinions and concerns of other colleagues. The final principle, principle 7, pertains to the software engineer themselves. The software engineer should participate in continual learning concerning the practice of this profession and promote an ethical approach to the practice of it. This includes improving their ability to make safe, reliable, and useful software at a reasonable cost and time frame. As well as furthering their knowledge in the fields of analysis, design, development, maintenance, and testing of software. These eight principles comprise the bases for a mature profession and although there are no equipments within the field requiring that they be followed, it is in the best interest of the public, client, employer, and employee to follow this code. They provide the backbone for acceptable ethic behavior for software engineers.

Chapter 9 [1] discusses topics involving Work and Wealth and includes many aspects of work and wealth. The first topic discussed is automation. Automation is the idea that machines are becoming more and more dominant in the workforce. This increases the production of other products which, in turn, creates jobs. We have already noted that robots are able to work longer, more efficient hours than the typical manufacture worker. This had led to a sharp increase in productivity in the United States. Information technology has forced workplaces to make changes. The first thing workplaces are changing is their organizational structure. Computers used to be used just for keeping the books. Now they are used for making very hard decisions. Because of the capabilities of computers, companies can effectively reshuffle their business scheme to compensate for utilizing cheaper computers. Telework is also changing the face of business. Telework is the ability for a person to work an office job from home. This lowers the necessity of an office, and office supplies for each coworker, saving businesses money. Studies show that telework improves productivity and attendance. On the other hand, telework downgrades the authority of managers. Now that people are working at home more regularly, it is important for companies to have stricter monitoring policies. Most monitoring devices are able to track all e-mail and websites the user sends and visits. The digital divide describes the fact that people who have access to modern technologies such as the internet have advantages over people that do not have these same technologies. The global divide is the divide that takes place when comparing countries. For example, access to the Internet is much more widely available in the United States than access to the Internet in Africa. The social divide is the comparison of people who have Internet access to people who do not have Internet access within a country. There are two models of technological diffusion, normalization and stratification. In the normalization model, the richest socioeconomic status is the first to adopt the technology, and slowly the middle and lower socioeconomic statuses adopt the same technology. Eventually there reaches a point when the technology is inexpensive enough for everybody to afford. The stratification model differs in that it fails to reach the point in which everybody is able to afford the technology. Companies such as Google and Yahoo! do not want a tiered service of internet access to be practiced. Companies such as AT&T want to enact different levels of internet access in which the higher paying customers get the best services. Google and other internet content providers do not want this to take effect because they believe that the Internet service providers will persuade their users to visit only their own sites by giving them better service to them. The "Winner-Take-All" society became apparent when information technology became more and more advanced. This phenomenon has existed for quite awhile in sports and entertainment. Globalization refers to the development of worldwide networks of markets and businesses. Globalization allows for a greater mobility of goods and services around the world. Advantages of globalization include: increased competition which results in higher quality products, job creation in poor countries, and the fact that two geographical areas are less likely to go to war against each other if their economies are dependent on each other. In contrast, globalization may not be favorable since all the workers in similar markets around the world would be competing with each other, regardless of working conditions. The Winner-Take-All phenomenon states that certain few people earn much more money for the work they do, than others who perform at slightly lower levels. Winner-Take-All markets can cause for a waste of talent; the high incomes of few high-profile lawyers have caused many intelligent college students to choose to go to law school, causing a shortage of nurses and nuclear engineers. In order to reduce the effects of a Winner-Take-All society, we must enact laws, reduce positional arms races, enact more progressive tax structures, and limit the amount of political power within the wealthiest percent of our population. People attend college so they can obtain a higher income. Studies have found that in the past 20 years, tuition at universities and public colleges has risen faster than inflation; the incomes of families have risen more slowly. Knowing this, we can conclude that a college education is more expensive now than it was 20 years ago. Plagiarism consists of using work or ideas of another person, and not giving them the deserved credit. Not giving credit to where it is due can have severe consequences. One should cite a resource if the information used was not common knowledge. Common knowledge is information that is readily available and known to many people. If one uses a direct quote from someone else's work, a citation is required. If one paraphrases the source document, a citation is still needed, but no quotation marks.

REFERENCES

1. Michael Quinn, Ethics for the Information Age (third edition), Addison Wesley Publication, 2009.

2. Narayan Debnath, Lecture Materials on "Computer and Information Technology - Progress, Challenges and Implications", Winona State University.