Addressing Ethics And Technology In Business: Preparing Today's Students For The Ethical Challenges Presented By Technology In The Workplace

Rochelle Brooks, Viterbo University and Capella University

The Computer Professionals for Social Responsibility (CPSR) web site provides us food for thought when they state, "Technology is driving the future, the steering is up to us.... and we need every hand at the wheel." (Computer Professionals for Social Responsibility, 2007).

So how do we prepare ourselves for taking the wheel as an individual working with Information Technology (IT) or Information Systems (IS)? Morality of respect doesn't appear, fully formed, at a particular age. Instead it develops, slowly. The story of that development is one of the great dramas of human growth, and one of the major contributions of developmental psychology to our understanding of children. If a child is brought up with care and understanding, then they will feel empowered to distinguish between moral or conventional issues.

The current trends suggest that the stages one goes through to build the foundation of good morals readily accepted into societal norms are in jeopardy. We have paved the way for more studies.

There is no question that starting young is the best time to address teaching good morals and ethics. But, that discussion needs to continue in our classrooms at the college level. Our students need guidance in making ethical decisions that are unique in today's technology-driven world. It appears that the more savvy we become in developing and using technology, the greater the risk that it will be used in a detrimental way against individuals, organizations, or society in general. We seem to be constantly struggling with new concepts that simultaneously present new opportunities along with new problems, or rushing to promote new legislation to counter some new threat, or redefining societal norms for our technologically-dependant world. Now is the time for philosophy (the study of ethics) and technology to meet. Managing computers ethically—that is, acting ethically and assisting others to do likewise—is no easy task for either an individual or an organization.

Samuel Johnson (British author in the 1700s, known as Dr. Johnson) once wrote that "Integrity without knowledge is weak and useless, and knowledge without integrity is dangerous and dreadful." (as cited Berkowitz, 2007). In fact, if you had to choose between living in a world of ignorant but caring, ethical people and world of educated and brilliant but selfish and antisocial people, which would you choose? I think it is a no-brainer. (Berkowitz, 2007). As Johnson noted, it is dangerous to educate people without a moral compass, or as former President Teddy Roosevelt once said, "To educate a person in mind and not in morals is to educate a menace to society" (as cited Berkowitz, 2007).

Is this a hot topic issue in today's society? Maybe the cover story of the October 29, 2007 ComputerWorld issue says it all in its title: "Ethics in IT: Dark secrets, ugly truths. And little Guidance." (Harbert, 2007).

According to Moor (1985), a typical problem in computer ethics arises because there is what he refers to as a policy vacuum about how computer technology should be used. It is evident in today's technology driven environment that computers provide us with new capabilities which give us new choices for action. In many cases, either no policies for conduct in these situations exist or the policies that do exist are inadequate. A goal of computer ethics is to determine what we should do in these cases. Computer ethics includes "consideration of both personal and social policies for the ethical use of computer technology" (Moor, 1985).

An example presented by Harbert (2007) gives us a reason to take notice. What Bryan found on an executive's computer several years ago still weighs heavily on his mind. He's extremely troubled by the male employee he discovered using a corporate computer to view pornography of Asian women and of children. This male employee was later promoted and moved to China to run a manufacturing plant. "To this day, I regret not taking that stuff to the FBI," says Bryan. This happened when Bryan was IT director at the U.S. division of a $500 million multinational corporation based in Germany (Harbert, 2007).

This company had an Internet usage policy which Bryan had assisted in developing with input from senior management. This policy—like most other corporate policies—prohibited the use of company computer to access pornographic or adult-content Web sites. One of Bryan's duties was to monitor employee Web surfing using projects from SurfControl PLC and report any violations to management. When the tools turned up dozens of pornographic Web sites visited by the exec's computer, Bryan followed the policy and went to his manager with copies of the Web logs (Harbert, 2007).

Bryan's case is a good example of the ethical dilemmas that IT workers may encounter on the job. IT employees have privileged access to digital information, both personal and professional, throughout the company, and they have the technical prowess to manipulate that information. That gives them both the power and responsibility to monitor and report employees who break company rules. IT professionals may also uncover evidence that a co-worker is possibly embezzling funds, or they could be tempted to peek at private salary information or personal e-mails. But there's little guidance on what to do in these uncomfortable situations (Harbert, 2007).

According to a security company known as Cyber-Ark Software, Ltd. a survey conducted during the spring of 2007 found that one-third of 200 IT employees who responded admitted to using their adminstrative passwords to snoop through organizational computer systems and peek at confidential information including salary. IT professionals admitted to snooping through confidential company information such as salary, personal e-mails, and human resources information as published in InformationWeek in 2007 (Harbert, 2007).

A poll of more than 16,000 U.S. IT practitioners conducted in June 2007 by the Ponemon Institute returned these equally disturbing findings:

- 62% of IT employees polled said they had accessed another person's computer without permission.
- 50% said they had read confidential or sensitive information without a legitimate reason.
- 42% said they had knowingly violated their company's privacy, security or IT policies.
- 32% of the respondents were at or above the manager level, and the average experience level was 8.4 years. (Harbert, 2007)

The Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices in business and government. The Ponemon Institute's services include industry-wide studies, proprietary (commissioned) tracking studies, training and consultancies on trends in privacy and data protection (The Ponemon Institute, 2007).

The temptation for curiosity is human nature, but at what point does it infringe upon unethical behavior? This needs to be discussed in our college classrooms. If students are being taught how to use the technology, shouldn't they also be presented with the ethical issues which the technology brings to the organizations in which they will be employed? Once employed, continued efforts of promoting awareness of ethical issues needs to be lead by management in our technology-driven organizations.

In terms of the many issues to study, we do have evidence to consider. Several major online news services were sampled in one week in March of 2004 by the Center for Computing and Social Responsibility to identify the current challenges that we face from technology. The results of the study promote the reason for providing an applied ethics education focusing on technology issues. Over 30 news items covered a range of problems and

focused on three perspectives: occurring incidents, technological countermeasures, and legislation. The news stories fell into several broad categories which are at the heart of the ethical issues (Rogerson, 2004):

Globalization: Controversy over offshore call centers and technology development in India (outsourcing) was included. In a range of articles about viruses, information access, and intellectual property theft, the underlying message was the extent and speed of impact due to the global nature of new technologies.

Intellectual Property: Microsoft was reported as aggressively continuing to protect its trademarks across the world. There were several reports on content theft. Peer-to Peer (P2P) file-sharing appeared in a number of reports. Parental obligation was under scrutiny in one report which revealed that many parents were either ignorant regarding the fact that swapping copyrighted files was illegal, or knew it was illegal but did nothing about it, or did it themselves after learning about it from their children. Finally, the music industry continues to worry about P2P and the fact it cannot control the Internet.

Identity Theft: The growing problem of identity theft is huge and identify theft is now known as the fastest growing crime in our society.

Viruses and Hacking: Computer viruses are destructive in our modern global society. Several viruses were reported during the study. Countermeasures were the subject of several articles. A new antivirus chip was reported in one, while one article recognized that hacking cannot be prevented and promoted the virtues of obtaining sufficient insurance coverage.

Junk Mail and Spamming: During the week of the study, China was reported as the second largest target for spam with one third of all emails being junk mail. Generally the abundance of junk mail has led to rampage in anti-spam software development.

Information Access and Denial: It was reported that China had closed two Internet sites used by many thousands of people because they carried content deemed to be objectionable by the State. A second report explained that TeliaSonera in Sweden had closed down a web site of the Islamic group Hamas because it violated the acceptable use policy. In contrast, one article centered on content filters to restrict access to information for school children to combat such things as plagiarism. Legitimacy of information services was the subject of a contrasting article on fake escrow sites.

Surveillance: Warnings were given about the need to be sensitive to employees' needs when implementing and operating surveillance systems. One article gave warnings about how every day accessories such as mobile phones were increasingly used for surveillance and that such intelligence gathering was commonly shared and condoned.

Health: Physical health can be at risk from technology. It was reported that those using multiple workstations were at greater risk of developing RSI-type injuries.

Conclusion: As the study shows, in one week the news has carried many ethical issues dealing with information and communication technology. According to Rogerson (2004), Director of the Center for Computing and Social Responsibility, *"A week may be a long time in computer ethics but if we do not address such issues the consequences will resonate for lifetimes."*

And why is all of this a challenge? Some feel that there has been a shift in focus from the "we" generation to the "me" generation. There will need to be a major paradigm shift before we can see ethics deeply engrained in every facet of our lives.

The technology itself makes moral and ethical decision making challenging. In some cases, the anonymity provided by information technology greatly reduces the likelihood of punishment, which is an important part of

early moral development. How would we choose to act if we became invisible; would we do whatever we want if we knew that we could not be detected, or would we still hold steadfast to our morality?

For more than a decade, the necessity of undertaking ethical issues relating to Information Technology (IT) and Information System (IS) development have been expressed and seriously debated by both philosophers and many concerned IT professionals.

Along with significant benefits of the Information Age come significant ethical dilemmas. Every day in the news, we can read and hear about issues surrounding intellectual property, data collection, improper use of technology and social implications, such as job displacement and unequal access across socio-economic levels.

As information technology professionals on the front lines of the decision-making, are they prepared to respond to these challenges? Are they even aware of them? Not enough of the IS professionals are aware. We have been so busy racing to keep up with rapid computing advances that we have not taken the time to address the larger societal implications.

The ethical development of information systems is but one of those sensitive scenarios associated with computer technology that has a tremendous impact on individuals and social life. The significance of these issues of concern cannot be overstated. However, since computer ethics is meant to be everybody's responsibility, the result can often be interpreted as nobody's responsibility. Therefore, an effective while still practical moral framework needs to be recognized in order to put computer ethics on a sound foundation for further exploration.

When ethical problems or issues related with IT/IS have been put forward and recognized, the most needed work is to find an effective way out of such dilemmas. Currently, among popular solutions are those that introduce codes of conduct and ethics, those that call for the relevant parties to give IS development procedures and products a secondary review, and those that focus on the importance of ethical training for practicing or potential IT professionals.

An area of focus in information technology is subsumption ethics. Subsumption ethics is the process by which decisions become incorporated into the operation of information technology (IT) systems, and subsequently forgotten. IT systems, by nature, repeat operations over and over. If those operations have unethical impacts, the system will continue to execute them anyway. Unlike a human operator, there is no point in the cycle where the machine pauses to ask, "Should I do this?" Subsumption, according to David Gleason (1999), in general is the process of building larger components from smaller ones. In this sense, a cell subsumes DNA function, American common law subsumes judicial decisions, and a hairdryer subsumes an electric motor. Subsumption in computers is different because there is so much more of it going on than in simple machines (Gleason, 1999).

In computer systems, small components are developed and tested, and once they are working reliably they are subsumed into larger systems. This is the enabling technique of object oriented programming. The larger systems, in turn, are subsumed into still larger systems. Once components, subsystems, and applications are operating, the subsumed process becomes invisible and unavailable to the user, what James Moor calls the "invisibility factor" (Moor, 1985). James Moor is a primary figure in the growing area of computer ethics. His award winning article, "What is Computer Ethics?" is widely reprinted and regarded as a milestone for the study of computer ethics.

Fundamentally, computer-based systems are little more than enablers for information misbehavior. Many of the newer information technologies enable persons to perform unethical or illegal actions more rapidly than in the past, to perform more clever or deceitful actions that might not have been manageable before the technology emerged, and to perform illicit activities without being easily identified. With computers and networks being so ubiquitous and accessible in today's workplace, the numbers of people who might knowingly perform an inappropriate act with them has grown rapidly.

Technology can help us to do things better, faster, and cheaper, and it can make us more competitive. On the other hand, appropriate, effective technology use in the workplace calls for new ways of thinking about things—new paradigms—and new ways of managing.

Many of the detrimental effects of information technology are caused by individuals or organizations that are not accepting the ethical responsibility of their actions. Like other powerful technologies, information technology possesses the potential for great harm or great good for all humankind. If managers, end users, and IS professionals accept their ethical responsibilities, then information technology can help make this world a better place for all of us.

It is time to become sensitized to all the aspects of information technology that involve ethical components. At times in the process of system analysis and design, we need to stop and say to ourselves, "There is an ethical dilemma here and I need to analyze it before I can move forward."

The author used this data to propose the creation of an Ethics and Technology class at Viterbo University in La Crosse, Wisconsin. That class was created. The author has had the privilege to teach an Ethics and Technology course at two universities with students ranging from traditional college age students to IT professionals making six figure incomes. What do students think about the subject matter? What are the hot topics? What is the foundation for teaching such a course? How to we prepare today's students for the ethical challenges presented by technology in the workplace? What type of impact does this type of course have on the people who complete the course? These are all questions that the author would like to explore and this is only a starting point.

When learners at Capella University taking a course entitled Ethical and Human Side of Information Technology are asked in Week 1 to describe the unique ethical problems in information technology and the reasons for studying computer ethics (cyberethics), the learners respond based on their experience and their views. Following are some examples of comments provided:

> I am a Network Engineer and work for one of the Intelligence Agencies in Washington D.C. Cyber ethics is now and will continue to be a hot topic in the news as well as in the IT industry. As the text suggests, there are many issues currently being explored in the area of cyber ethics from individual anonymity in cyberspace to the illegal distribution of intellectual property. In particular since September 11, 2001 a battle has been waging over the governments right to monitor ISP chat rooms and email versus each Americans individual right to privacy. Both sides of the argument have legitimate points and clearly highlight our struggle as a society to define what is ethical in the cyber realm.
>
> Other issues that jump out at me are the ongoing problems dealing with software and copywrited materials in cyberspace. This affects Americans more than they think. As companies experience loss of revenue in sales, they pass that loss onto the consumer, both to make up for the loss of sales as well as to help off set the cost of research and development.
>
> There are many more issues such as employers monitoring their employees email and web browsing during work hours, all the various types of computer hacking, and disinformation being passed across the internet. All of the issues stated above and the ones I didn't mention have a direct impact on most of our lives. The arguments over what is socially and morally right in the cyber realm will continue as the global society attempts to define cyber ethic boundaries and laws.

Another learner focuses on the invisibility factor in his reply:

> I think CyberEthics is a valid arena to exist on its own because of the unique issues that it addresses that don't necessarily exist elsewhere. I found Moor's essay on this to be very succinct at touching on many of these issues. The primary issue I see is that which Moor calls the "invisibility" factor or the way in which computers and the technology involved with them

> behaves almost always behind the scenes, and this can make any activity by a computer suspect to biases in programming, intent of the user, intent of the administrator, and a host of other issues. The fact that, in regular ethics there is generally visible proof of what was done and at least some revelation as to why it happened that way, whereas, with computers and the information they deal with, as Moor says, everything is malleable. This is what gives computers their power, but the perception we receive does not always lead to truth or fact. Sometimes this is desirable, and sometimes not, and in that rests the problem.
>
> As more information that is important to our finances, our personal identity and other vital parts of our existence in society becomes involved or enmeshed with this type of technology for convenience of transmittal, storage, or what have you, the fact that data can be changed makes our personal information possibly subject to such a change. Whether it be our social security number, or a program that we have made and intend to sell, or a sensitive email that we would only want certain parties to see, data integrity, Confidentiality, and availability becomes a concern for everyone as more of this information becomes accessible to others and can be altered/distributed by those who have the know how and access. This involves property rights, information privacy, personal identity, as all of these things are now touched in major ways by computer technology. These three particular issues I think are what make Information technology ethics, or cyber ethics, an important distinct set of ethical issues.

One woman in the class used some comparisons involving using the Internet vs. not using the Internet which shows a definite difference in thinking:

> Ethics and technology is a hot topic issue that very few people understand the consequences of. The internet gives a level of anonymity that is nonexistent in the unplugged world. Cameras and time stamps record our every movement on this country's grid and most every person is aware, but when it comes to the Internet, where anyone can become someone else, it seems as though many people compromise their normal ethics. The average person would never think about going into a store, breaking into a glass case, and stealing a high end program, but many people have no problems obtaining a cracked version of that same program on the Internet and using that. They wouldn't think about stealing a CD, but downloading hundreds of thousands of songs for free is somehow justifiable. Copyright infringement, identity theft, and privacy invasion are all realities of the digital world that people who wouldn't think about doing the same action to a person they can see have no problem doing it to people they'll never know. I find the ignorance about the consequences of abusing the invisibility factor, copyright infringement, and data theft to be intriguing since there seems to always be an excuse for whatever the case may be.

One learner who works as a professional web designer shares his interests as follows:

> Cyberethics is something I have been interested in for a long while. Being that I am into web design knowing exactly what not infringement is and what is, is very important. Such as designing a website similar to another one that works well if that is legal or even ethical. Also what steps can be taken to stop infringement on copying of work. I find our legal system not caring really. I think it is more of a generation gap of what's "real" and what's not. I think any company that develops software that doesn't before as agreed to they should held liable. I expect the new car I buy to start and better believe I am going to take it to the company and make them fix the problem.

Another learner has a solid focus on ethical issues involving technology in the global environment:

> In an ever increasing global community, our world becomes ever so smaller. A dichotomy of epic proportion where a wire can connect two or more individuals living oceans apart. The problem lies where one border recognizes a set of rules while another does not. I am interested in this cross

> border issue where ethics in technology play a big role on what is disseminated and moved globally.
>
> Some people ignore or just plainly do not know that copying an MP3 or perhaps a DVD is punishable by law, US law that is. Other countries might be more tolerant of such behavior. And while software developers spend large amounts of money protecting their intellectual properties to prevent such behavior, once across international boundaries the threat of fine and imprisonment is severely diminished. In the end it is up to the individual who has rightfully purchased such media to keep from redistributing such information.
>
> James H. Moor writes "Computer ethics is not a fixed set of rules which one shellacs and hangs on the wall." I concur and go a step further in noting that the study of applied ethics is society centric. You'd think it was a simple question of right or wrong. Not so… what is acceptable in one culture or country might be completely counter-intuitive to another. Ethics in technology will continue to be an ever evolving, ubiquitous field of study and argument as is the computer itself.

One learner raises a case for the idea that "ethics is ethics" regardless if technology is involved or not:

> I don't know as I think there are ethical problems in information technology that are 'unique'. Theft? Breaking and entering? Dissemination of secrets? Unauthorized copying of information? None of these problems are particularly new. They may be easier to get away with, and appeal to a less daring group of people, but unique? Not particularly.
>
> I don't really see much of a distinction, which may be a generational thing, but as someone who has lived online since there was an 'online' to live in, none of the ethical considerations raised in the reading strike me as being particularly unique to information technology. Cesar had passwords. What is a credit card but a password to an account? The Vestal Virgins had data storage issues and privacy policy violations, and lost a great deal of customer data after their takeover… by the Hun's. In later times Payne's "Common Sense" may have been more pirated than Spears 'Oops I did it again', and Dot bomb CEOs with low standards are probably no scummier than those who made up the original Silicon Valley boom of the gold rush. And as for piracy… where did we get the word pirate!?!?
>
> Perhaps if, as the Woodbury (his wife, not the farmer) article implies, we are the same ethical 'you' wherever you are, then your ethics needn't be specially applied any more in computers than they do on the highway, or in airplanes.

And, if there was a negative learner in the group, it would be this one:

> No one knows the evil that lurks in those boxes called computers, but be afraid, be very afraid. Since the beginning of time there have been slime balls who try to circumvent the system, any system not just this new technology but any and all. Now, thanks to that great inventor, Al Gore, we have new problems to think about.
>
> Slime balls always lurk in the shadows, those areas like alleys are now computers and the slime wants to get your kids, your money and everything else you have that they can get their hands on and use to get their kicks.
>
> Our text book (cyberethics) talks about the "invisible factor" and how it is basically a double edge sword because on the one hand it helps us remain unknown and unseen to an extent, and it is also possible for software developers to mix in little surprises in the software they make, legitimate software and not so much legitimate, but innocent looking malware but harmful in some ways that

> the average person does not now realize. I am trying ever so hard to get pumped up and enjoy this class and I hope all of you do as well.

In contrast to the negative view, this learner presents a positive outlook on how technology can be used to solve problems:

> I was immediately drawn into the Cyberethics book, especially when I read the Introduction, about how Sue was really Bill in an online chat room. In my opinion, the internet allows people to jump into a vast sea of endless stuff. Anything can be pulled up in Google. This is helpful, but also, scary. I remember discussions when I was in junior high about kids using the internet for research. If a student would type in certain words, pornographic websites tied themselves to those words, making it easy for kids to view their websites. There are also internet watchdogs though, who fight to stop that sort of thing from occurring.
>
> I think that anyone who works with computers today has to be an observer, like Aristotle, and observe all the processes going on around them. At my company, we use the computers to get the jobs done. But now as the aging computer processes are looked at today, with new updated technology, we are asking ourselves - How we add value to our processes? We try to find problems with current processes. The solutions to those problems are found by getting thoughts and idea's organized. We then ask, how can we apply any technology we have available to solve these problems? We always try to digitize and automate as many repetitive manual processes as possible, which saves our company both time and money.

Invisibility and privacy were key focus areas in this discussion and this learner expressed his view of ethical problems very clearly:

> I think one of the biggest ethical problems in information technology is anonymity. The freedom that computers provide by allowing people to create any persona they want is kind of scary. I also think that people who create programs receive a certain level of anonymity as well. You may have a name, but more than likely you know nothing about this person and what they've actually programmed the software you are using to do behind the scenes. I think both of these situations fall directly under the invisibility factor.
>
> The invisibility factor can provide people of nefarious intent the avenue to steal information from just about anyone who uses a computer. This is why I think studying ethics and what part they play in the world of computers is beneficial. By being aware of both the negative and positive ways someone may use a computer it can help reduce the chances of people being taken advantage of.
>
> I think a second ethical problem in the world of computers is people's belief in their right to privacy on the internet. I think anyone who thinks that what they do is guaranteed privacy through email, blogs, news feeds and online storage are fooling themselves. I do not think there is anything unethical about a company that provides a service such as email or web hosting having the ability to look at any file or folder located on their hardware anytime they wish. If you don't want people to know your business... don't put it on the internet.

The next step in my research is to more clearly evaluate the outcomes of taking a course in Ethics and Information Technology. In my study of learners I wanted to track change in attitudes, if any, at the end of the course. This will require future research and an additional time commitment. The author hopes to be rewarded a research fellowship which would provide some resources to continue research in this very vital area of study.

It is the author's hope to develop a survey to gather more data but following are some contrasting comments from two people completing the course. Following is from a learner who is trying to figure out for himself why this content is so important since he already knows it IS important:

> As I continue through this course, I understand why the study of ethics is so important and then wonder just why is it so important? With multitudes of codes, cultures and just plain individual thinkers, it becomes quite perplexing. The "Hacker's Code" for example states that all information should be free, mistrust authority, etc, compared to "Using the Code of Ethics" which illustrated a librarian's trials and tribulations of pornographic material accessibility and the code that she was "required" to subscribe to as a professional. On one hand one states that the information should be freely available and the AMA code could support such. The other hand quickly slaps down and takes the position of degradation to women of the next generation or perhaps the use of public dollars for this type of material as being misguided.
>
> Take the example a bit further; pirated software can easily be shared across the Internet. The Hacker's code would make this perfectly acceptable. The AMA code and the ever so regimented ACM code of Ethics would frown upon such. The Computer Ten Commandments might even light a bush on fire. What to do?
>
> I don't know, I'm ever more perplexed over codes and really respect those who can think for themselves and do the right thing or the left thing. Do well by another and treat one as one would like to be treated.

In following the discussions of the learner who commented about slimeballs being both online and offline, it was easier to understand his initial comments when he shared the following at the end of the course:

> After reading the assignments and then finding other codes of ethics and reading all of those as well, it is apparent that they are extremely well thought out. They are documents that try and take every possible angle into consideration. Collectively, whether it was a code of ethics for lawyers, engineers or social workers they all had one theme that stood out, and that was how they are supposed to treat each other and all of the people that they may come in contact with while doing their respective jobs.
>
> Those codes of ethics will be very helpful in the process of putting my team's code of ethics together. The number one premise in them all is how coworkers and peers should treat each other and the customer and we will keep that in mind as we proceed with our own code of ethics.
>
> The older I get the more I appreciate people and I try to be cognizant of how I treat them all. It was not always that way though as my family was primarily small minded bigots so I had to overcome that little obstacle. I suppose my point is that we all probably develop our own little code of ethics throughout our lives. I know that was not part of the assignment but I did it anyway. I am living on the edge today baby.

According to Harbert (2007), in theory, ethical behavior is governed by laws, corporate policy, professional ethics and personal judgment. But as IT pros experience in their jobs, this can be one of the most overwhelming challenges in their careers. Perhaps it would ease Bryan's conscience to know that he did just what labor attorney Linn Hynds would have advised for this case. "Let the company handle it," she says. She recommends to make sure you report violations to the correct individual in your company and to provide the evidence. She feels that you then need to leave it to the people who are supposed to be making the decisions. Ideally, corporate policy should take over where the law stops in governing workplace ethics to clear up gray areas and remove personal judgments from the equation as much as possible.

Another example shows the need for continued concern. When Tim, a systems administrator, discovered an unencrypted spreadsheet of salary information on a manager's PC, he copied it. He states that he didn't share it or use it to any advantage. His reason for taking the file: "I just took it to prove that I could." Tim's actions point to a disturbing trend: IT workers justifying their "ethically questionable behavior" (Harbert, 2007).

"Moral good is a practical stimulus; it inspires an impulse to practice" (Plutarch 40-120 A.D. as cited by D.B. Reinhart Institute for Ethics in Leadership, 2007). "Whichever side of the line they're on, IT professionals will—for now at least—continue to muddle through ethical dilemmas on their own and wrestle with their consciences afterward" (Harbert, 2007). What can be done to help and is it enough?

REFERENCES

1. Berkowitz, M. W. (2007). Social and emotional learning. Committee for Children. Retrieved November 21, 2007 at http://www.cfchildren.org/issues/sel/education/
2. Computer Professionals for Social Responsibility (2007). What is CPSR? Retrieved August 15, 2007 from http://www.cpsr.org/
3. D. B. Reinhart Institute for Ethics in Leadership at Viterbo University (2007). Ethics in leadership research fellowships. Viterbo University.
4. Gleason, D. (1999, March). Subsumption ethics. *Computers and Society*, 29, no. 1. pp. 29-36.
5. Harbert, T. (2007, Otober 29). Ethics in IT: Dark secrets, ugly truths. And little guidance. *ComputerWorld*. Vol. 41. no. 44.
6. Moor, J. (1985). What is Computer Ethics? *Metaphilosophy*, Vol. 16, No. 4, pp. 266-275.
7. Rogerson, S. (2004, April). A week is a long time in computer ethics. *IMIS Journal* Volume 14 No 2. Retrieved October 19, 2007 from http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/Ecv14no2.html