T1 - The economic value of information by Kent Harvath

Since computers and internet developed a wide informational system, much information than ever has been available on internet. Though most of the information is free here, it is reasonable that in such environment, there are people who try to make money out of information on internet, creating a market for information on internet. There had been market for information on books, but internet has made it easier to access information and increased the number of information accessible, and therefore greatly affected the market for internet and the economic value of information. Some people consider this information economy to be the next phase of economy following hunting, agriculture, and manufacturing economy.

The market has now been entirely on internet. They advertise the product on internet. The customers look at it on a web page. They order it through internet and the purchased information is sent completely as data, many times called e-book. There also are numerous articles that charge money to read. The value of information has increased for both business people and customers. Information is now a profitable product. It is also suitable for earning money because the production cost is almost zero. It does not cost to duplicate the information because it is purely data, and there is no need to hire workers. This not only increases the profit, but also decreases the risk which is not a problem if it does not sell well. The fact that the price of e-books are actually high (above $10.00) regardless of low cost suggests that the demand is high as well. ebook prices

Thus, these people involved in the internet market for information benefits from this increase in economic value of information. The people who suffer from this are people involved in old market of information such as books. Due to the law of substitutes, the demand for books results decreased by the increase in demand for e-books.

One social issue that may occur by the increase in economic value of information is that economic value of other products may lower. Despite the increase in economic value, information itself is useless in many circumstances. It can not substitute for food, stationary, houses, or any other things that form the basis of our living. Since it is easier and much more efficient to earn money by information on internet, many businesses would concentrate on information, and the competition for other field would be less and incentive to innovate would be lowered in that area.

Though this internet market on information seems to be very efficient, there are problems that could occur within it. One problem is anonymousness. It is easier to deceive people. Much information could be plagiarized information. Also, in many cases, advertisement on the web page makes the information look to be really useful, and the price may be very expensive, but the information itself is really poor. The problem here is unreliability. So many things are unclear on internet that these social and ethical problems arise. Due to the fact that the information economy is just in the stage of development, there still aren't many laws that regulate these problems yet.

Another ethical problem that arises is black markets of information. An example would be a list of e-mails sold. It could be a list of e-mails of people who are interested in certain things and people buy it to send advertising mails. Or it could be a list of e-mails of not intelligent people who got tricked by some information product which is purchased by people who intends to trick people. Anyhow, the development in informational network also encourages this kind of trade as well.

Thus, the economic value of information has increased due to development of computers and internet.

T2 - Environmental issues related to the disposal of obsolete hardware and computer supplies by Roger Maue

1. What are the issues associated with this subject?

There are issues that concern the computer's parts or components which caused a certain amount of pollution or environmental effect when manufactured. Such a component is the hard polymer or metal cover that protects the computer chips, computer boards, computer systems, etc. When computer components are manufactured, it is first extracted as a natural mineral which when discovered in huge quantities can lead to cutting down of forests or other natural surroundings which affects the natural habitat. It is then taken to be processed then delivered to be chemically tested using hundreds of chemicals (many toxic, complex, and changing-mix) to a certain durability which if not controlled the gaseous mix can leak into the atmosphere can cause air pollution. Or simply the land needed to build a factory to produce the components can lead to more destruction of land which supports a large ecosystem.

2. How did this technology emerge?

The problems emerged when manufacturers first started to develop large scale production of computers once the technology to build cheaper computers emerged and also the ability of the average consumer to purchase it increased too. Thus it was set that the consumers were willing and able to buy the product which was supplied by the manufacturers who could produce it in large scale due to efficient, fast, low-cost, and innovative ways to produce the computers. But the environmental issues that could arise from it was not at first noticed by them until later on when the dots were finally connected that the manufacturing methods or materials or what was done to extract, create, and finally the later disposal of the used product in a environmentally safe storage place.

3. Who are the stakeholders?

The people most related and take blame are the companies who during its early years thought of this technological and profitable breakthrough as a new page in technological history which they saw and probably thought of it as excellent way to change the world and also to boost our understanding of computers and its help to society in helping building it up. It must have been good and very profitable to have the computers out on sale to the masses that could purchase it. But they didn't realize that the emissions from the factory or the product's certain materials could have environmental effects and eventually they could be at stake as one of the main causes of these problems since they were mainly the ones to blame since they had initiated the computing manufacturing industry.

4. What are the advantages and disadvantages for those stake holders?

The advantage for the stakeholders is that they can say that the during those times they didn't know the side effects of manufacturing the components of the computer and the process in creating them involved a lot of destruction or causes to environmental problems. They could argue that the technology or knowledge that could have helped detect the side effects were not in existence or that their equipment weren't environmentally safe.

But the disadvantage for the stakeholders is that they will have to plead guilty to not conducting further research on what kind of side effects their manufacturing of the components could have. Also they could be accused of merely focused on the profit side of things that they didn't look into the side effects or that they didn't want to let the consumer know in fear of a rejection of their product. It could be possible that the cost of making adjustments to make improvements to their product could cost a lot so they could face a lot of disadvantages and be in a lot of trouble.

5. What solutions can overcome the problem?

The solution to overcoming or solving the problem could be easier because of the technological advance in helping solving environmental problems and our knowledge and expertise has grown. It could be solved step by step or all at once simply by starting with the manufacturing site which can be solved by using old unused work areas that are far from the environment, reselling or upgrading computers to save energy, better extraction of natural resources by experts and better instruction of future disposal of the product and improved manufacturing ways and better research, extending the lifespan of computers to reduce environmental effects, banning of extremely toxic substances and proper use by the consumers.

6. What areas of impact does it affect?

Even though it is not regarded as a major problem when the computing world is discussed, it still stands a problem that affects many sectors of society because it can cause problems economically for when companies try to cut costs of production many people can lose their jobs for now it is a major multi-billion dollar industry employing thousands of workers so their cut could mean drop in the economy which can lead to other problems. It can also benefit other sectors such as the environment which is key issue that is worked to improve by computer manufacturing companies.

7. Evaluate the impact locally and globally.

There is always an impact it will have both locally and globally because the computing world is right now a key part in today's world for it helps shape and make the world change so for ex: if IBM has one of its manufacturing units shut down for manufacturing a certain component of the computer such as computer chips as outdated by a newer chip then IBM will let its branch in China at a certain similar manufacturing unit to shut down for their current product is outdated. Locally and globally the economy can suffer for loss in jobs for the IBM employers and also the consumers.

8. What are the ethical issues?

The ethical issues are that it there is great harm caused by the manufacturing companies to the environment that activists would probably say that the environment provided the materials and then they are polluting in return and that other innocent citizens of the world could suffer from the side effects in the environment besides humans which include the animals. It is very sad that this effect on the environment could endanger certain venerable animals and in some cases humans too.

9. Who is responsible?

To an extent the average computer owner or future one is to be blamed because it is through them that they bought the computer in the first place in his/her own choosing and reason that they have made it clear that there is a demand or that another of the computer units has been sold. But also to the ignorant distributors of the product who didn't consider the side effects or try to at least provide inputs or precautionary knowledge to their customers.

10. Who is accountable?

The individuals that can be held accountable are the manufacturing companies and its management who were probably for not responsible for not letting the general public or its customers know of what their product was capable of environmentally causing side effects and it was them who manufactured the product and should know its pros and cons and let the public know of it or at least make it clear of what it do.

11. What laws apply?

The companies found guilty could face the court by Department of Forestry, Greenpeace, etc. or other organizations or individuals or groups that are affected. There are laws which govern the companies' esp. on their output on environmental emissions or other forms or environmental harmful wastes that there are regulations, procedures, and guidelines that mistakes are criticized and punished. The laws are subdivided into specific branches such as aerial pollution, land pollution, and water pollution and so forth.

12. Are there alternative decisions?

Other methods that could be taken to improve the problem is that governments could increase the tax system on price tags, smoothen transfer of software licenses with used equipment, and setting up free blue book for used computers. While the distributors could ask the firms for not only price and quality, but also environmental performance and they could with the firms to start incentives to set up collection/resell divisions for old computers and its components for proper professional disposal.

13. What are the consequences of these decisions?

Governments would not want to increase taxes for it could be the county's main economic provider and other methods will be unlikely to be passed out by the government or it might simply cost extra money which the government wouldn't want to spend. It might take a long time to get off and work effectively and people won't want to be taxed or it could be that the consumers might cause the firms to demand a change on the order by the government for it is losing a lot of money so it could cut workers and cause an economic shortage on jobs. Or skilled workers could leave the country to make a better living overseas so the human skill could be on a shortage.

T3 - Password protection, Security, Biometrics and Authorized access by Akira Jackson

First of all, what are password protection, biometrics and authorized access? Password protection is a form of security that uses various numbers, alphabets and symbols to prevent other people from accessing your computers and private files. Another form of security that has emerged recently is biometrics, which uses various body parts, such as eyes and fingers, to identify individuals authorized to view confidential company information.

The issues surrounding these subjects mainly concern the hackers and other people who try to get through the security that is set up. For example, hackers can figure out passwords using various programs and tools or by simply guessing. Also people believe biometrics is a form of protection that they can rely on, but nothing is perfect; even biometrics can have flaws.

For example, in the case of face recognition the machine uses the information like how your face is shaped, the location of your nose, ears and their shape. In this case people can use a realistic model of the person to fool the machine, or coerce a person with access privileges to allow entrance. Voice recognition can be fooled using high-quality recordings or simply forcing the individual to speak in front of the machine to get in.

That goes for authorized access as well, which mainly uses passwords during login to determine if the user is granted authority. This also can be broken easily and even altered so the original user is unable to control the computer. Also people from the company can be paid to get individuals through security, or fooled by social engineering specialists. For example, Kevin Mitnick, a former hacker, regularly convinced people over the phone that he belonged to the same company and obtained passwords from them. So there is nothing that can keep you completely safe from outside interference.

I think one solution to help overcome the problem would be to make the punishment heavier for the hackers and other individuals that try to get past various security measures. Also companies can hire hackers to check if their security is reliable. Another way to overcome the problem is to hire security personnel, who would be useful because they can recognize people that do not belong to the company.

What areas do hacking and other illegal behavior affect? First of all, the economic consequences are huge. This is because hackers can break in to various companies computer and steal new technologies and company secrets. Then they can sell these secrets and technologies to rival companies and even other countries, which can greatly impact society because companies would lose profit or gain profit that they don't deserve. Also, people's sense of security would be greatly affected because there is always a possibility that someone would hack into your computer and steal or mess up documents and files.

The act of looking at people's private files and documents is ethically wrong, and destroying or stealing them is even worse. This is mainly because they don't belong to you and because the individual didn't permit you to look at the documents. In cases of stealing company secrets and new technologies the same logic applies. You don't deserve the technology if you didn't acquire it through your own efforts. Faking the biometrics is almost the same as saying you had criminal intentions because outside of the entertainment industry there is no need to copy other people's faces, fingerprints, voices and so on in everyday life. Breaking security means you are getting into somewhere you don't belong and ignoring other people's thoughts and feelings, which is morally wrong as well.

If you break into a house by faking the biometric security is entering the house without authorization, which is against the law in Japan and many other countries. Also, if you hack into a game CD and copy the content and resell the copies this is against the law on copyright. The main law concerning hacking and accessing files through hacking is the law that states: knowingly accessing a computer without authorization and gaining

information and this is what some hackers do. Most of the other laws state the same idea like intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage Most laws deal with individuals who break into computers without authorization and steal information from the computer. But it is bit in the grey area if the individual only breaks the protection but does not cause damage, steal information, or copy files.

T4 - Issues related to viruses on both stand-alone and network systems by HeeJun Son

In these days, every computer is very vulnerable to computer virus. Internet is everywhere. As the world is connected by the network system and computers do all the things for people, the economical damage caused by the computer virus is immense. Not only computers control the business system, but they also do control the transport and traffic systems. If the computers are harmed by the viruses, the consequences will be enormous as many news articles tell us a lot of people get disadvantage from the viruses.

1. What are the issues associated with this subject?

As they became existing everywhere, viruses have become the major problems in these days. They replicate themselves in the computer and alter operation system without any owner's consent. People even get their information stolen and viruses utterly destroy a computer. There are many kinds of viruses: boot sector viruses, companion viruses, email viruses, macro viruses, cross-site scripting virus, etc. They are programmed to damage the computer by altering programs, deleting files, or reformatting the hard disk. The viruses have bugs leading to data loss or more serious problems. Malwares are slightly different from viruses although most people assume they are the same things. Malwares are made to destroy a computer system. Trojan horses and worms are the common examples of malwares.

5. What solutions can overcome the problem?

The easiest way to solve the virus problem is not to allow the virus to spread out of control at the first place. Unfortunately, in the Internet, it is harder to prevent viruses from sneaking in. The anti-virus program may be one of the good choices to get rid of viruses from the computers. However, it also removes a good virus. The problems of this kind are traditionally more difficult to solve than the technical ones. However the anti-virus softwares may help greatly to solve those problems associated with destroying the computer system. And we should not install any suspicious program on our computer.

8. What are the ethical issues?

It is unethical to change other people's data without their permit. Computer viruses change the information on the computer. Therefore they are illegal and unethical. Some viruses having malicious intent can steal personal important information and erase the whole data in the hardware. Sometimes the stolen information can be posted on the web. If that is a case, anyone is possible to see his or her personal important information. Anybody who sees that on the web can abuse it. Thus the virus problems have caused ethical issues.

9. Who is responsible?

Many people believe that only a few people who have great knowledge of computer programming can create computer viruses, perhaps like an intelligent computer programmer. But creating virus is not as hard as most people may think if you properly understand how the program works. People make viruses because mainly they want to feel the thrill or to show off their special talents. If a person knows how to make programs, he or she will easily make destructive viruses that spread very quickly. People create the viruses because they also want something beneficial from someone. As we can see the people who are good at programming and have a bad purpose are responsible the problems of viruses

T5 - Greater dependence of organizations on IT by Takafumi Kurihara

My topic would be about the greater dependence of organizations on IT systems. First, what is IT. This is the contraction of information of technology. These are use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information. With these, we are able to gain information from many places within few minutes or few seconds.

The ability that we can get much information really quickly makes us depend on the IT system more. One reason is that we people tend to want information more quickly. Another is that when ever human are wondering, they would like to find them out quickly as possible. These two mentalities make people depend on the IT systems more than before. Then there would be questions like why people want to know things quickly or find out an answer. Well one answer would be that we want to satisfy or feel some happiness towards getting an answer to everything. Another would be that we would be able to decide which decision would have a higher possibility to success. And the last would be the efficiency towards ever single thing.

Another large thing is that it is really easily done. Many people, especially young people, like to depend on easy works. They would find out the way to use the IT system and use them to make their life easier. This makes people able to get information around the world real time and make their work smooth and easy.

Last thing would be that we would depend on the system too much that when ever the systems gall down, we are not able to gain any information. Another would be the efficiency would go down a lot and the whole other system that humans made, traffic, train, stock exchange, and other more would stop moving and there would be a big disaster.

This totally brings us that we would depend on the IT system now, but we would depend on it more. One is that it makes our work smooth and easy. Another is that we are able to learn a lot of stuffs through the IT systems.

T6 - Increase in teleworking and the virtual office by Sung-Hwan, Chun

Telework is a work arrangement where the employees don't have to come to a central place of work. Instead, they commute and work using the telecommunication links. These telecommunications include not only internet as general, but also telephone, fax and video. But, usually the Teleworking is relied upon by the internet.

The virtual office is an internet office which allows clients to use using internet instead of using a physical office. This usually takes the form of websites and the customers could further communicate using fax, telephone, e-mail, and virtual meeting rooms.

Using Telework reduces the distance restriction of using a central place of work. The use of Telework would benefit largely to the employees who live far away from a central place of work, because this saves significant amounts of travel time and cost. Also, it allows more employability of parents with small children, and the handicapped.

Teleworking is seen as a solution to traffic congestion, because the employees don't need to ride a car or train to come to the central place. Therefore, the passengers of train and road congestion at rush hour would be decreased. This would reduce the air pollution by decreasing the use of cars. Finally, by using Telework the employees could enjoy a great amount of freedom. In other words, the employees could relax in their sofas at home, with a warm coffee cup in their hands, and having a rest when they want. There will be no employers to constantly pressure, the only thing the employees need to do is do the assignments given by the employee.

One would think that the main problem with this kind of Teleworking would be the management of employees. How would the employers know that the employee is doing their work, not playing around? The common solution for this is to give an assignment with a due time. For example the employer would sign an employee to type up 500 words essay by lunch. Then, the employer could check in at lunch by e-mail or by other telecommunication to see if the employee has finished it.

Therefore, the employer can't check the real progress of the employee, so the employer doesn't know whether the employee was playing around 'till last hour of the lunch and finished the 500 words essay or whether the employee took all its time to finish the essay. But, this doesn't really matter because all the employer wants is that the assignment is well-written and done. If the assignment was not done, then the employees would find themselves unemployed.

The major problem however, is the security and the management of the telecommunication to work properly. There might be problems caused by miss typed information, for example, the employer giving wrong assignments to wrong employee, or giving 700 words report instead of 500 words. Although this could be solved if the employer is cautious, it is a common mistake occurring because it is easier to make a mistake when we are using a machine rather than using our mouth.

The malfunctioning of the telecommunication would also be a big problem. For example, if the internet was down, then, the employers would have a trouble sending the assignments or information to employees. Or even worse, if the employee's computer got a virus and it erased all the reports he wrote, and then he would be fired because employer thought he didn't finish the assignments. This would be very unfair for the employee, and the reasoning out that he got a virus would not really work, because the employer might think that the employee is blaming it on the virus. The solution to this is to maintain a high security system, which would cost the employers, and also to maintain better telecommunication devices.

The virtual office would have all the advantages the Telework have and also saves the employer a lot of money, because the cost for a central office is not required. The virtual offices have a productive customer services through telecommunicating, which is efficient and comfortable.

The problem with the virtual office though is that the intranet access to the telecommuter may be slow due to telephone or modem connections. Use of groupware, browsing, and downloading also may be slow due to the same reason. Therefore, the customers might face great discomfort using this.

The solution to this is difficult, because this is dependent on the connection speed of the customers. Therefore the company might lose some of the customers because of this.

T7 - The need for ongoing training and retraining by Andrew Leung

What are the issues associated with this subject?

The main issues associated with this subject the ever increasing amount of viruses, trojans, bugs and all sorts of computer problems that come up when the user is in use of the computer. These problems are forever increasing and evolving in a sense that they progress and get worse every time it happens again. That is why there is the

need for constant training and retraining of computer technicians and assistants to help solve these problems. Computer engineers also try to solve these problems by trying to make non-faulty and highly protected systems that cannot be attacked or damaged by viruses and trojans.

Who are the stakeholders?

The stakeholders of this issue are the users of the systems that are constantly being attacked by the creators of the trojans and viruses or the random bugs and computer problems. The users are the people who potentially loose all their information on their system through these problems that may arise. With these problems that could occur on certain systems, they might not occur on another system resulting in a higher popularity of the system that does not seem to have as many problems. As shown in the following graphs, when problems arise in one system, (Figure 1) the demand drops for that system. Then if the same types of problems don't arise in another system, (Figure 2) the demand for that system goes up.

What solutions can overcome the problem?

Solutions for overcoming this problem with trojans, viruses, bugs and computer problems would be the training and retraining of new ways to solve the problems. This training and retraining goes towards computer technicians and assistants who help users through the problem of their computer. Computer engineers on the other hand are trained and retrained to create systems that make the existing problems not to be able to arise from the start. With the nullification of these problems demand for the system goes up gradually.

Evaluate the impact locally and globally.

All computer users are affected by these problems presented above. These users are mostly the people in industrialized countries where the person is capable of owning their own computer or system. On the local scale it could possibly be one problem that arises within the network of a workgroup. A problem could arise in one system which could possibly be passed on to the other systems that are connected to the system with the problem resulting in all local computers to be harmed. On a global scale, the problems usually arise through the passing on of trojans and viruses through the internet from one source which is usually unknown.

Who is responsible?

The people that are responsible for trojans and viruses are crackers or "dark-side hackers". Crackers are people who are malicious and criminal hackers. These crackers are people who exploit their computing genius for private gain. Unlike crackers, hackers are highly skilled computer programmers who make programs and software's that help other users that are not as experienced in computers. Hackers also can make already designed software's and programs work beyond their normal limits.

Nobody can be accounted for creating bugs and technical computer problems because the computer engineers, who had created the system, would have run tests that passed the tests of their standards and therefore did not know of the bugs or problems that could arise when a user experiences the problems. That is the reason for the engineers to train and retrain to find ways to fix and prevent these bugs and problems from ever arising again in newer systems.

All in all the training and retraining of computer technicians and assistants are done to help technicians and assistants help the users of the systems that are experiencing problems with their computer being it trojans to a simple bug on the system. The training and retraining of computer engineers is to give them the information of what new problems there are and what they can do to prevent the new threat or problem. Then when the new systems are made, it makes it harder and harder for crackers to exploit the newer more sophisticated system.

T8 - The economic and psychological implications of planned IT obsolescence in hardware, software and services, which has been forced on consumers by the IT industry by Sam Shobeiri

In our day and age, technology improves everyday. As technology improves, the computer industry is able to produce better hardware, software, and services. What results from this is that companies are able to produce newer, updated programs within a short period of previous release. Even though the fact that technology improves helps to improve our daily lives, it has some problems that needs to be addressed.

What are the issues associated with this subject?

The issue here is that as companies in the computer industry produce new software, hardware, and service, they are to a point forcing the owner of an older software or hardware to update. As technology improves, standard of specs and functions increases. Therefore if you do not update your hardware and software, you will not be able to be interactive in the society as there will be compatibility issues. Those with newer software, hardware will be able to open data that comes from a computer with older software and hardware, but many times, not the other way around. Often, companies will stop offering technical support to older hardware and software, making customers tempted to buy the newer version. Is it right for the companies to almost force the customers to update and at the same time charge ridiculously high prices for their products? Shouldn't customers that bought the older products be equal to the ones that bought the newer product and get the support they need?

Who are the stakeholders?

The stakeholders here are the computer companies producing software, hardware, and services and the consumers who buys them. The companies believe that by producing better, newer programs as much as they can, they are helping technology to improve and create easier and more advanced society. On the other hand, even though consumers like the fact that the technology is improving, most are not attached to a point where they keep on buying newer products. They argue that companies are producing updated software and hardware that creates limitations for older software and hardware, which almost forces the customers to buy the newer versions.

What are the advantages and disadvantages for those stake holders?

One advantage for companies in computer industry to produce new, updated software is that they are improving technology and contributing to the society. Also, obviously, they are making more money by producing updated products. Disadvantage for the companies to make updated software is that if there is not much difference from the previous one, the product will not sell. Advantage for customers to upgrade is that the performance of the product increases, which increases efficiency and quality of whatever task the product is meant to do. The disadvantage is that they will have to keep on paying ridiculously high prices for every upgraded products.

What solutions can overcome the problem?

There are two solutions to this problem. It is not reasonable for anyone to say that the computer companies shouldn't produce upgraded products as improvements are always welcome. The problem here is not the fact that companies are upgrading, but rather the price and lack of support for previous versions. It would be ideal if upgraded versions were free of charge, but as that is nearly impossible, they can at least in case of software reduce the price of upgrades for those that own the previous version. In this case the consumer can buy the newer product for smaller cost and therefore be happy and the companies are still making money. Also, to keep the customers of the older software satisfied, the companies should keep on providing customer and technical support.

Who is responsible?

Obviously, the ones responsible here are the computer companies. It is good that they are always improving their products, but by forcing an upgrade and charging high prices, they are making it tough for the consumers.

Are there alternative decisions?

There are few alternative decisions that can be made in this case. Either do not upgrade at all, or, in case of software, download illegal copies of the upgraded version.

What are the consequences of these decisions?

The consequence of not upgrading at all is that you fall behind in this fast paced world. By not having the latest hardware and software, you can be very limited in what you do. A lot of things possible in new products are not possible in the old ones, causing compatibility issues. The consequence of downloading illegal copies is that, obviously, it is illegal. If you get caught, you get thrown in jail.

T9 - Organizational policies and standards, for example, e-mail, surveillance and monitoring policies by Matthew Wilder

How did this technology emerge?

Network surveillance and monitoring policies have been used primarily by corporations and governments to spy on employees and civilians. By using such policies to monitor computers and networks, corporations check whether employees are doing things that are work related, and governments gain information from individuals that interest them (i.e. terrorist suspects).

Such electronic spying methods have emerged ever since everything started to become computerized. Groups that spied realized that it was a lot easier to hack into computers or check internet acces history rather than send people, actual spies, on investigations. Thus, computerization brought along a whole string of network surveillance methods, from different kinds of hacking to various spy programs.

What areas of impact does it affect?

Evaluate the impact locally and globally.

The biggest area of impact concerning organizational network policies is privacy. With people you don't even know searching through your computer, the idea of privacy in the modern sense is negated. Furthermore, the more recent surveillance technologies allow for a person using the technology to be completely undercover, and so the person being spied would never even know that he or she was being searched. In this sense, privacy is affected.

On a local level, network policies will affect people at the workplace, or for students, at school. In the case of a student, network policies may prevent the student from accessing certain contents on the computer (i.e. porn, games). In the workplace, like for the student, network policies may prevent people from accessing certain contents like corporate secrets, but policies also track what you have been doing on your computer.

For example, in many companies, the company will filter your internet history to see whether you have been accessing websites that are unrelated to work. When the company does find something unrelated, the company then uses that piece of information against you. The sole purpose of this is to increase productivity, the idea being that monitoring policies will create an incentive to only do work related activities. On a more global and larger perspective, surveillance policies are used by government agencies for spying.

An example is the Chinese government, which has a department solely created for the purpose of browsing through the internet to look for websites that state things that go against communist morals.

Who are the stakeholders?

What are the advantages and disadvantages for those stake holders?

The biggest stakeholders in the usage of organizational network policies are usually, in the case of corporate network policies, the lower ranked employees. In a company, it is usually the people at the top, the management, that apply monitoring policies, and the people below that are monitored. Thus it is almost always the people at the lower end of the social ladder that are affected. These people are the ones who are fired when their managers find out that they have been spending hours on Youtube. A major disadvantage, as previously discussed, is that these people lose a lot of privacy when such policies are put in tact.

The advantage of taking away such policies on the other hand, are extremely clear; stronger privacy and freedom. Of course in some ways the people on the other side are stakeholders too. Without such policies, managers would not be able to assure shareholders of the company that their employees are being as productive as possible. With governments, network surveillance is extremely valuable as that is how a lot of information is gained on people. The disadvantages of not using network policies, for these groups, are all too apparent.

Who is responsible?

Who is accountable?

The people responsible and accountable are the corporations and governments that decided to use organizational network policies. These groups were the ones that started developing such policies and they were the ones that had the incentive to do such things.

What are the ethical issues?

What are the issues associated with this subject?

The right question to ask when the implementation of network policies are being debated is, is it ethical to search through a person's computer without the person's consent? The answer to this is, like the implementation of such policies, is debatable. On one hand, you could say it is wrong because doing such a thing is in a way, a violation of one of the more modern human rights; privacy.

Spying on one's computer will destroy the person's privacy. Of course, if the person was playing computer games at work all day, then you could say in that case spying is justified, but what if the spy accidentally opened up a private email that showed the person was having problems with his wife? The person most probably would not want let anyone know about that, yet the network manager now knows.

A question you could ask yourself then is, does the network manager have any right to know about the person's marital problems? On the other hand though, you could say that the infringement of privacy is justified. CEOs of a corporation might justify his use of monitoring policies by saying that the computers his employees work at all belong to the company, and so thusly, the company can do whatever the company wishes to do on the computers.

CEOs may also say that they have to assure stockholders that their workers are being as efficient as possible and that productivity is at the highest level, and to ensure that, the company has to make sure people are only doing work related tasks on their computers. So as you can see, privacy is a big issue associated with this subject.

What laws apply?

What solutions can overcome the problem?

Governments around the world usually have laws that allow for the government to pursue a policy of network surveillance. For example, in the Unites States, under the Patriot Act, law enforcement agencies are allowed to search through people's computers without a search warrant. In China, the Communist Party constantly passes new laws that allow for the government to spy via the internet.

So what solutions can overcome the debate over the usage of organizational network policies such as surveillance? One possible solution to the problem at hand is to allow for network policies, but not make the policies unknown to people. People could be given reports each month or so on the history of their computer usage for that month. This will especially work in the workplace because employees will know that they are being checked for, and they will know exactly what the employers know about them. This solution will still provide an incentive for workers to stay on task while at the same time lowering the level of privacy intrusion in the sense that the workers know which aspects of their activities are being inspected.

Are there alternative decisions?

What are the consequences of these decisions?

Other than the solution stated above, there are few if any, alternative decisions to organizational network policies other than to not use such policies. But again, there are consequences to this alternative, much of which hit the people who implement the policies. Without computer surveillance, managers will not be able to ensure productivity in the company and governments will have to use more inefficient and difficult methods to gain intelligence.

Knowledge of technology

In order to study and evaluate the social and ethical issues involved in the use of IT systems, the student must have an understanding of related technological concepts. These may include:

T10 - Key Terms

Data, information, hardware components, for example, input devices, output devices, processing, storage, memory (RAM, ROM), MHz, dpi, bit, KB, MB, GB, TB, ASCII, compatibility by Tommy Chuang

Peripherals, Platforms, Firewall, Malware, Computer Worms by Xiao Xiao

Verification and validation, encryption/decryption, virus, Trojan horse, Logic bomb by no one

In order to be able to understand the social and ethical issues of information technology, one must have an understanding of technical terms.

An input device is any device that puts data into a computer. One example of an input device is a keyboard, because it is used to input commands for the computer to follow.

An output device is a device that is capable of taking information from a computer and representing it visually or audibly.

A computer monitor would qualify as an output device because it gives a visual display of the information in a computer. For example, a word document is nothing but data on the computer's hard drive, but the monitor displays it in a way that allows humans to read it with ease.

Processing is the act of performing operations on data, such as making a calculation with a set of numbers.

Storage is the capacity of a device to hold and retain data. Devices with larger storage are able to hold more data, and devices with smaller storage are not able to hold as much. Over the years, the amount of storage that devices have has increased at a phenomenal rate. In just thirty years, devices have gone from being able to store 128 bytes to 500 gigabytes.

There are two types of memory: RAM and ROM. RAM stands for Random Access Memory. It is a space where data is written so that it can be accessed by the CPU. It is only temporary, however, so once the computer is turned off, any information that was stored in RAM will disappear. Word processing documents such as Microsoft Word often store unsaved information in RAM. ROM stands for Read Only Memory. Unlike RAM, ROM is permanent and cannot be removed. A computer's ROM sector will typically contain information that is vital to the computer, such as what to do when the computer turns on, or what operating system to use.

ASCII stands for American Standard Code for Information Interchange. It is a standard code that is used for creating and encoding text documents so that they are viewable by any program. An ASCII text file will not contain any special embedded control characters. In ASCII, every number, letter, and symbol is assigned a special code, called an ASCII code. A capital A, for example, has an ASCII code of 65.

Because operating systems often are programmed very differently, programs may have varying degrees of compatibility when run on different operating systems. For example, there was a time when Microsoft Office was compatible with Windows, but did not run on Mac computers. Also, programs may experience compatibility issues with different versions of the same operating system. A program designed to work on Windows XP may not work well with a computer running Windows 95.

OCR is an acronym for Optical Character Recognition. It is the ability of a computer to recognize text that is printed on an image instead of an actual text file. An example of this is having a book scanned into a computer, and then having the computer be able to recognize the image as text. From then on, it is possible to edit the text with a word processor. In order for OCR to work, some sort of optical scanner is required to feed the images into the computer.

OMR stands for Optical Mark Recognition. It is technology which involves reading data from marked fields. An example of OMR is in an application form or voting ballot. The answers for the form are written down on the paper in a marked field with a pencil, and an optical scanner then reads whatever is printed in the field and interprets it before feeding the data into the computer. Another example of OMR is the bubbles on SAT tests. These bubbles are read by an optical scanner and fed into the computer.

Bar code is a way of representing the UPC, or Universal Product Code, so that it can be easily read by machines. The UPC is a 12 digit number assigned to products. It's purpose is to identify the product and the product's

vendor. Bar code represents this code in a series of black and white bars, with the widths of the bars signifying individual digits in the UPC.

A baud is a measure of the number of bits that are transmitted every second. Higher baud indicates a faster transfer rate, and lower baud indicates a slower transfer rate.

Peripherals, Platforms, Firewall, Malware, Computer Worms by Xiao Xiao

• Peripheral is a type of computer hardware that is added to a host computer in order to expand its abilities. The term also tends to be applied to devices that are hooked up externally, typically through some form of computer bus like USB. Typical examples include joysticks, printers and scanners. Devices such as monitors and disk drives are not considered peripherals when they are not truly optional, and video capture cards are typically not referred to as peripheral because they are internal devices.

• In computing, a platform describes some sort of framework, either in hardware or software, which allows software to run. Typical platforms include a computer's architecture, operating system, or programming languages and their runtime libraries.

• A firewall is an information technology (IT) security device which is configured to permit, deny or proxy data connections set and configured by the organization's security policy. Firewalls can either be hardware and/or software based.

• Malware (Malicious Software) is software designed to infiltrate or damage a computer system without the owner's informed consent Many normal computer users are however still unfamiliar with the term, and most never use it. Instead, "(computer) virus" is used in common parlance and often in the general media to describe all kinds of malware.

• A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other systems and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

In order to fully examine the social and ethical issues surrounding the use of IT systems, an ITGS student must first grasp the various technological concepts as of above. Assuming everyone is already on top of the more basic terminologies, valuable time and space should be spent on exploring the more intrinsic technology concepts such as malware and the tons of issues surrounding this sensitive topic.

One of the most notorious forms of malware is Trojan horse, a malicious program that is disguised as legitimate software. They may look useful or interesting (or at the very least harmless) to an average user, but are actually harmful when executed. There are two common types of Trojan horses. The first is an otherwise useful software that has been corrupted by a cracker inserting malicious code that executes while the program is used.

The other type is a stand-alone program that tricks the user into some misdirected complicity that is needed to carry out the program's objectives. Either way, the areas of impact created are huge. With the prevalence of global internet access today, everyone is a potential stakeholder. What makes it even scarier is the fact that everybody can also be potentially responsible and accountable for this infringement of morality. All it takes is one mentally “corrupted” individual for a global internet contingency to occur.

A simple example of a Trojan horse would be a program named "waterfalls.scr.exe" which claims to be a free screensaver. But in reality, when operated, it begins erasing all the files on the victim’s computer, raising distinctive ethical issues. However, this isn’t all. When Trojan horses are being utilized on a larger platform, such as firms, serious social issues also begin to arise. One type of Trojan horse is logic bomb, a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

For example, in June 1992, a defense contractor General Dynamics employee, Michael Lauffenburger, was arrested for inserting a logic bomb that would delete vital data. It was alleged that his plan was to return as a highly paid consultant to fix the problem once it triggered. Fortunately, his dream plot was shattered when another employee of the company happened to stumble upon the bomb before it was triggered. Lauffenburger was charged with computer tampering and attempted fraud and was ultimately fined $5,000 plus jail time.

However, stakeholders shouldn’t count on luck or the law to protect them from the dangers submerged in the IT world. After all, it’s important to keep in mind that internet is still a lawless “cyber space” connecting people around the globe and that Trojan horse is only one of the many “villains” among the different types of malware. Hence, alternative solutions should be preached instead. After all, the good news is that Trojan horse programs cannot operate autonomously, in contrast to some other types of malware, like viruses or worms. In fact Trojan horse programs actually depend on actions by their intended victims.

Therefore, Trojan horses can and should be protected against through user awareness.

Firstly, since Trojan Horse viruses are most commonly spread through an e-mail, as an e-mail user, one should always confirm the source. If one receives an anonymous e-mail or one with an unknown attachment, avoid opening it directly with the use of an anti-virus program that scans the attachments. Furthermore, make sure your computer has an updated anti-virus program regularly. Finally, although tempting and hard to resist for

teenagers, the use of peer-to-peer or P2P sharing networks such as Kazaa and Limewire should be avoided because they are generally unprotected and especially venerable to Trojan horse viruses.

Although some of these programs do offer some virus protection, but they are not nearly enough against the overwhelming odds. It is only when everybody works in accordance towards preventing and fighting malware such as Trojan horse can the resultant ethical and social issues be alleviated.

T11 - Use, advantages and disadvantages of analogue and digital data by Tomer Lapidot

Today, most of technology is presented both analogically and digitally. Digital data is considered any data that is transferred or stored in the binary form of 0 or 1, while analog data is data in the form of continuous electrical waves which represent an infinite amount of values. The main advantage of the digital data over the analog, is that once recorded, digital data never looses quality once copied, and can be copied infinite amount of times maintaining the same quality, unlike analog data, which although can represent infinite amount of values, data is deteriorated after each copy of it that is made.

1. What are the issues involved in ITGS?

2. How did this technology emerge?

The ITGS industry is one that digitalizing. The digital technology is what is considered more modern, and with better quality. Since information in processed through computers, more information becomes digital. Digital technology emerged with the creation of computers, since computers and chips where the fist machines that worked with a binary base, and thus, stored their data in a binary base. As computers get more powerful, the quality of digital data improves. Computers with today's computing capacity can already digitize photographs and sound to a level high enough that the human eyes and ears can not distinguish between digital and natural sound and an analog or digital picture anymore. Analog technology however has been around for longer period of time. Ever since the creation of the radio, telephone, and television, information was sent in the form of electric waves, or stored on magnetic strips. However, if not the original recording was used; the quality of the data would decrease and would not be nearly as good as the original.

3. Who are the stake holders?

4. What are the advantages and disadvantages for these stake holders?

Digital and Analog data is around for everybody. Computers, televisions, radios, watches, music player, microphones, speakers, telephones, are all items which fall into analog or digital data. The transfer of electric data is an integral part of modern society; society can not exist without it. The choice between choosing a digital device or an analog one falls into two categories, money, and fashion. Since digital is synonymous with quality, example, digital video camera, digital speakers, digital television broadcasting, these become luxuries which are to be purchased at higher prices. Thus, quality is a function of money, and that quality is based on digital technology. Fashion, however, is based on analog systems as it is on digital, for example, expensive wrist watches tend to be analogical, showing the time with the classic hands instead of LCD digits. However, in the practical utilitarian sense, digital technology is superior, and thus, costs more.

5. What solutions can overcome the problems?

6. What areas of impact does it affect?

7. Evaluate the impact locally and globally.

Since the social issue of the digital and analog market, is directly related to money, the more money one has, better quality he or she can enjoy. The major impact on society of this issue is that the more digital a person is, the higher his or her economic status is. Thus, richer people will enjoy digital technology more than poorer people. And so, anywhere in the world with a civilized society can an electronic industry.

1. What are the ethical issues?

2. Who is responsible?

3. Who is accountable?

Since digital data can be copied any number times without loosing quality, copying becomes easy. This property became abused by sharing and peer to peer programs such as Kazaa, Napster, and eMule, where copying music illegally is done easily. The product of copying digital music files endless for everybody cause the artist, and in the picture, the market to loose millions of dollars. Is it ethical to steal music over the internet just because technology can allow it? Such peer to peer file sharing programs reached global dimensions, can millions of people all over the world are responsible for abusing digital music's ability to copy, and the composers lose money.

4. What laws apply?

5. Are there alternative ethical decisions?

6. What are the consequences of these decisions?

Clearly, copyright laws come into play when copies can be made as easy as they can with digital data. Because it is only logical that stealing someone else's is not ethical, because a creator deserves credit for his or her work. An ethical decision would be simply to enjoy digital recording technology's quality, while respecting copyright laws. Such decision may be harsh on young adults or teens, who can not afford luxuries like digital sound or vision quality, and peer to peer programs appear as a solution for not paying money for music and enjoying the same quality, but it would protect artists and their rights.

T12 - Operating systems (multitasking, boot) and utilities, for example, defragment, disk format, virus scan programs by Xaio Xaio

There are two major operating systems today – Windows and Macintosh. Both of these operating systems can perform the tasks listed above. I'll go in details on how each operating system performs the tasks listed above and many others.

First, and perhaps one of the main tasks is multitasking. Multitasking refers to being able to perform many tasks at the same time. For example, listening to music on iTunes while working on a document or watching a movie while creating a PowerPoint slideshow. Both Windows and Mac can perform this. And switching of programs is very easy. In Windows, you can just press Alt+Tab while in Mac you have to press Apple+Tab to switch between the programs.

Boot refers to starting up the computer. From experience, Mac OS starts at a faster pace than Windows. After the computer has been started, you can click on "Start" buttin in Windows OS to start working and for Mac, just go to Finder or search for whatever you want to use in spotlight.

Utilities just refers to "useful programs" that in computers' case help the computers run more efficiently. This is where the main difference comes between Windows OS and Mac OS. While in the case of Windows, you HAVE to use all these utilities in order to make your computer run smoothly, in case of Mac, none of this needed. Why? It's just because of the basic infrastructure of the two operating systems.

In windows, disk defragment and disk formatting should be done once/month so old files are processed properly and new files are more accessible to the user. If this isn't done then the computer becomes slow because it takes more time to access the old files. If this is done, then the computer is "relatively" faster because the old files have been defragmented. Formatting of the disk refers to preparing a hard disk for use. This is needed when the operating system is corrupt or there's a virus in the system. Then the formatting of the disk should be done so that the virus is taken care of and the disk is ready for use again. Both of these are not needed in Mac OS because Mac automatically keeps a record of all the new files that are created and hence the spotlight function is much more faster than the search function in Windows.

Now the last thing: virus scan. As we all already know, Windows has about 114,000 known viruses while Mac has…none. Yep, that's right – Mac has no viruses and hence none of the anti-software stuff is needed for Mac. A Mac user can just use his Mac while not worrying about any spyware or virus cleaning his/her hard drive. Windows users, however, have to be on a look out for possible viruses all the time. That's why windows users spend all their money on extra software to keep their computers running smoothly! Conclusion is buy a Mac and use the computer for what it was made for! Be happy!

T13- Responsible computer use (for example, regular back-ups, virus checking, security, storage, housekeeping) by Raymon Ohmori

Backups. They are almost required in this day and age if you have important, irreplaceable data or even just your normal, everyday data. Take this hypothetical scenario if, say, your data was on sheets of paper in real life; if the safe in the back room of your house is where you want your data to be, then most of your data is on the front porch, or, if you have a decent firewall (Windows Firewall does not count as decent), it might be on the floor in your entryway. Maybe, if you encrypt it, it will be on the desk in your room or under your pillow, but nothing will be in that safe. If your house gets robbed, if your house burns down, if your house gets toppled like a one-pole tent in an earthquake, or even if your house gets bombed by the Chinese, chances are you've lost that paper.

And how do you get stuff into that safe? Backups. Everything can fail these days. Your hard drive is the most likely, but your whole computer could fail, and if you're running a company with servers, your main server could fail. Say your college thesis was three words from being finished, and your hard drive fails. If you did not have a backup, then you might as well have handwritten the whole thesis and then tossed it in a campfire before handing it in.

We often do not make backups – it takes time, its a boring, repetitive task, and it feels like meteor strike insurance – never needed and totally useless. In fact, however, it's more like health insurance. It doesn't seem needed, but there comes a day when you're quite glad you got it. However, backups are still time-consuming. There are automatic backup systems available, but they cost an arm and a leg and them some. However, excellent and fairly wallet-friendly backup methods do exist.

Most likely the easiest way to do an automatic backup is to create a RAID1 or RAID0+1 hard drive array. RAID0 is data striping across two hard drives, which means blocks are placed on alternating hard drives, thus combining two hard drives into one big one with essentially double the speed. The problem with this is that if one hard drive fails, both fail. All is lost. RAID1, on the other hand, is data mirroring. This means that when ANYTHING is written

to the master disk, the second disk writes the exact same thing. Thus, if one hard drive fails, you can pop the other one into the slot and you're home dry. However, is a virus comes and rips up the one hard drive and corrupts all your data, the second one will happily copy all that over and your backup is lost. Finally, RAID0+1, as the name suggests, is a combination of RAID0 and 1. You have four drives, two each striped and one set mirroring the other. This combines the wonderful speed and space of RAID0 with the safety of RAID1, but it fills up all your hard drive slots and viruses will mangle four drives worth of data.

If you are part of a large corporation, then you are better off with expensive backup software. This way, the copying of viruses can be avoided and backups are still non labor-intensive. However, the backups only stay current as long as you keep updating them; if you only perform a backup once a week on Friday and a hard drive fails on Friday morning, then you are set a week behind. The process of backing up large quantities of data is hard-drive usage intensive, so if you perform backups too often you will be in the middle of something and then your computer will slow down to a crawl. If your corporation uses servers or the like, you probably want to backup not just the data, but the entire server, so that when the server goes down another will fill its place while it's getting fixed. This is called redundancy – the replacement doesn't even have to be as powerful as the main server; it just has to keep things from grinding to a halt. Google never goes down because they probably have an insane amount of server redundancy spread out all over the world so they stay online even if a cataclysmic disaster wipes every datacenter west of Chicago off the map.

Finally, you instead of buying a safe, you could buy alarms, cameras, tripwires and maybe even motion detectors and laser tripwires to catch any robbers stupid and unlucky enough to choose your house as his (or her) next target. Just like this, you could install security systems on your computers and servers. In this way, you can protect yourself against any malware; viruses, trojan horses, spyware and keyloggers will not be a threat to the wellbeing of your data. Then again, there have been many cases of these things getting past security, so this method is not perfect. That's not all – just like how you have to step over or deactivate your tripwires when you want to go somewhere, security systems in your computer can be an inconvenience. Norton Antivirus™ , for instance, is infamous for slowing down your computer, and other programs block things that you don't want blocked. And on top of all these problems, security won't protect you against a hard drive failure.

It's better to shell out $3,000 for a good, fireproof safe than losing 50 grand worth of money and important documents in a fire or a thief. In the same way, all these problems and expenses with backups are still better than losing all your data and getting fired if that data was your employer's. A wise man once said, “You can fix the idiot in the computer, but you can't fix the idiot at the computer.” You can keep the computer from crashing and screwing up, but you can't keep the user from screwing up and that includes the user not backing up things that are important. I admit that even I do not perform regular backups; in fact, if my computer exploded right at this very instant, I think I would lose half of all the torrents I've downloaded and most of the recent additions to my website. And yet, even as I admit this, I don't think I will perform a backup tonight as it is late and I have more interesting things to do; my hard drive hasn't made any alarming noises yet.

T14 - A responsible and systematic approach to implementing or upgrading IT systems, for example, analysis, design, implementation, testing, evaluation, training, policies and standards by Romeo Wu

Information Technology will be one of the key factors driving progress in the 21st century it will transform the way we live, learn, work, and play. Advances in computing and communications technology will create a new infrastructure for business, scientific research, and social interaction. This expanding infrastructure will provide us with new tools for communicating throughout the world and for acquiring knowledge and insight from information.

Information technology will help us understand how we affect the natural environment and how best to protect it. It will provide a vehicle for economic growth. Information technology will make the workplace more rewarding, improve the quality of health care, and make government more responsive and accessible to the needs of our citizens. Information Technology also deals with the design and use of computers and communications for solving a wide variety of problems. It is remarkable that computers, which were only developed about 50 years ago, are now used in such a large number of large organizations.

We accept as part of our normal life that almost all bills and payments from governments and large organizations are printed by computers and that services such as Medicare or Bankcard are possible only because of the effective use of computers. Although the applications of computers are diverse, from printing bills to controlling a blast furnace, they all require that information be stored in the computer and manipulated by computer programs.

There are two main category of Information Technology. Data management comprises all the disciplines related to managing data as a valuable resource. The official definition provided by DAMA is that "Data Resource Management is the development and execution of architectures, policies, practices and procedures that properly manage the full data lifecycle needs of an enterprise."

This definition is fairly broad and encompasses a number of professions which may not have direct technical contact with lower-level aspects of data management, such as relational database management. Data storage is a system for recording information. Recording can be done using virtually any form of energy. A storage device may hold information, process information, or both. A device that only holds information is a recording medium. Devices that process information may either access a separate portable recording medium or a permanent component to store and retrieve information.