Week - 5

Q.1. What are the four ways professional ethics differing from ethics in general? (8 marks)

Answer:

General ethics are essential personal values and code of conduct that we self-create. Ethics in general are applicable to whole society. Every person living in the society should follow them to make the society a habitable place, in simple terms a good society. ex., respecting elders, helping someone cross the road, not to steal from anyone, help an accident victim by taking him to hospital etc. These are not our moral duties but ethical duties which we owe to society at large. These involve your morals and values. They satisfy your personal needs; they only influence your behavior with people you know personally. They are instilled generally, during childhood, by your parents, family, and friends. They relate to your deep-rooted principles, and how religiously you follow them determines the kind of person you are. The nature of your personal ethics depend on whether your principles have an optimistic effect on the people surrounding you, i.e., your strict adherence to your principles must not spoil someone else's life; a negative impact on society due to your principles violates the very reason you are following them. They rely only on the individual. They are designed by the person himself, to make his life more orderly and disciplined, and he depends on them to define his life.

Examples

Sincerity and honesty fall more under general ethics.

I will always speak the truth.

I will respect all those who are elder to me.

I will never hurt anyone purposely.

I will maintain a caring attitude towards everyone.

Professional ethics are values introduced by and organization or professional company. Professional Ethics is a different ball game; they vary from profession to

profession. They are a part of your job and helps you to maintain the credibility of your company as they help the company making an image for itself in market. At the time of training they hammer down those ethics in you. ex, reaching office on time, not cheating or misleading your client. If you are working in a restaurant or hotel than a cardinal work ethic is “The guest is always right”, etc. In japan the average delay of the bullet train is less than a minute, they achieve this feat because of their work ethics (punctuality). One more thing every profession has its ethics, even thieves and contract killers, assassins have them, ex., they never divulge the information of their employer and once taken a job they always complete it. These involve a strict code of conduct laid down at the workplace. They satisfy your corporate needs. Your professional career is influenced by these rules, and the more stringently you follow them, the better professional you will be. Your ethics here involve adherence to rules and regulations. Non-compliance to such rules may risk your reputation, as your behavior will immediately be reported as brash and unprofessional. Your personal views and concerns about any topic will not be of much help in a corporate setting, how well you follow the protocol of the company is what will matter here. They rely on the organization. They are formulated and laid down by the organization, and they need to be upheld by whoever works there, irrespective of his designation or salary.

Examples

Confidentiality is an example of a professional ethic value.

Punctuality

Time Management

No Gossip

Safeguard Company Privacy

Q.2. Write a short 300-word essay related to the discussion question. Your team is working on a computer-controlled device for treating cancerous tumors". You are behind schedule, the release date of the device to your customers is rapidly approaching and there is not enough time to complete the planned testing, should you release or continue testing? Try to follow the methodology for making ethical decisions discussed at the beginning of the tutorial, i.e. the brain storming phase followed by the analysis phase. (15 marks)

Answer:

Consider that your team is building a machine designed to save lives, but if it malfunctions, it can kill or injure patients. Delivering the system on time benefits the company but could endanger the patients. We must analyze the case further. We need to identify the affected people (or stakeholders). Firstly, the patients who will receive treatment with the machine. A malfunction could cause injury or death. Secondly, there is an impact on the hospitals and clinics who will purchase the machine. Delay could cause financial losses to them. Third one is, your decision affects you and your company. Negative consequences of delaying delivery could include damage to your reputation for managing a project and loss of other contracts, resulting in reduction of jobs for the company's programmers, developers and other employees. On the other hand, if the system injures a patient, the same negative consequences are likely to occur. This brief examination shows that delivering the system without complete testing could have both negative and positive impacts on patients and also on the manager and the company. We assume you are honestly trying to weigh the risks of delivering the system against the costs of delay. You, as a computer professional, have more understanding about the complexity of computer programs and the potential for errors, especially in programs that interact with real-world events such as operator input and control of machinery. We assume that careful thought went into devising the original test plan for the machine. You should delay delivery and complete the tests.

Some patients will benefit from on-time delivery. The machine represents an improvement in medical treatment, but there is no ethical obligation that it be available to the public on a certain date. You are not responsible for the disease of people who rely

on existing treatments. Your obligation to the people who will use the machine is to be sure that it is as safe as good professional practice can make it, and that includes proper testing. You do have an ethical obligation to use your professional judgment in a way that does not expose people, without their knowledge, to additional harm. What about your responsibility to your company? Even if we weigh the short-term effects of the delay more highly than the risks of losses that would result from a malfunction, the ethical arguments are on the side of fully testing the machine. Yes, you have a responsibility to help your company be successful, but that is not an absolute obligation. Your responsibility to the financial success of the company is secondary to ethical constraints. In the present case, avoiding unreasonable risk of harm to patients is the ethical limitation.

Q.3. A television manufacturer has hired your company to develop a personalization system using a camera on front of the television set and face recognition software to suggest programming and to target ads to the individual watching TV. What risks to privacy does this entail? What features should you include? How should the system or TV Company inform buyers about the system? If the system recognizes that two people are watching television, which one's profile should it use to recommend programs or select ads to display? (15 marks)

Answer:

Facial recognition is one of the easiest and most commonly used biometric tools. It is a subcategory of biometrics. It's made possible by advanced computing components, such as processors and memory, and Artificial Intelligence (AI) tools, such as machine learning. Facial recognition is when a device uses a camera to identify a face for security or other purposes.

When it comes to public safety, however, the technology has had a tentative (not certain) roll-out. Consequently, facial recognition software can be faulty when mapping and matching faces of people of color, women and the elderly. The racial element is especially troubling, particularly in the countries like: United States (US). Black men and queer (odd or strange) women of color are disproportionately (unequal) imprisoned compared to other populations. An inaccurate facial recognition software has the potential to further that inconsistency; moreover, it could lead to a higher number of mistaken identities due to false matches. Regarding ethics, issues have arisen in areas from necessity, complicity, impartiality, bias, accountability and oversight. Some software developers are not comfortable developing the technology for public safety. Many concerns surround the issue of privacy. Who will own facial image data? How will police and public security team share this information? Will it be securely stored or vulnerable to malicious actors? Facial recognition data can easily be collected in public places – all the software would need is a clear image of the subject's face. It is hard to recognize the accurate face in the busy and crowded public places. Even if recognized it may be more than one which results in false recognition. So for that new technology must be introduced that helps in effectively recognizing the face even in the most crowded areas as well.

Q.4. A factory manager has hired your company to develop and install a surveillance system in the factory. The system includes cameras small enough not to be noticed. Supervisors and security personnel can view images in real time on monitors in a control room. The system will store video. The factory manager says the purposes are to watch for safety problems and for theft of materials by workers. What issues, specifications, and policies will you discuss with the manager? Would you set any conditions on taking the job? Explain. (15 marks)

Answer:

Many employers use cameras and video surveillance in the workplace, often to prevent theft or to monitor what employees are actually doing. Because filming can implicate privacy rights, however, employers must be very careful not to cross the line. For example, there might be a video camera that tapes everyone who comes in the door or stands in front of the register. But what about employers that use hidden cameras to try to catch their own employees stealing? What about video surveillance of employees while they're working? Or cameras in the bathrooms or locker rooms?

Filming employees at work is legal depends on the stated law and on what images are being captured. Privacy is a cherished (treasure) value for most of us. Even if your state hasn't passed laws that specifically protect workplace privacy, you almost certainly can't tape or film employees while they are doing certain things at work, such as using the restroom or changing clothes. If there's no state law that specifically allows or prohibits surveillance, courts determine whether an employee's privacy has been violated by looking at two competing interests: the employer's need to conduct surveillance and the employee's reasonable expectation of privacy. An employee who is using the bathroom or getting undressed has a very strong, and very reasonable, expectation of privacy -- and few (if any) employers will have a substantial enough need to justify filming employees doing these things.

Other activities may also be off-limits for employer surveillance. For example, employers may not secretly film or tape union meetings. A court could well rule differently if an employer's surveillance (observation) strayed into private activities and effectively

deterred (discouraged) employees with a legitimate (legal) need for leave from exercising their legal rights.

Q.5. You are the president of a small computer game company. Your company has just bought another small game company that was developing three new games. You find that one is complete and ready to sell. It is very violent and demeaning to women. It would probably sell a million copies. You have to decide what to do with the game. Give some options, and give arguments for and against them. What will you do? Why? (15 marks)

Answer:

Regarding the development of video games, we did not find female characters represented as forward and aggressive. Many of these images of aggressive female video game characters glamorize and sexualize aggression. Enormous female video game supporters have emerged, and some have speculated that this indicates new power and liberation in the image of the female video game character. We, however, agree that aggressive female figures that are also objectified, sexualized and dominated are not true figures of liberation. The capacity of being everywhere of aggressive females, and especially of sexualized aggressive females in video games, is a very important development. Traditional theories relating to the role of gender in society stress the importance of male aggression and dominance. Researchers should continue to investigate media depictions (portrait) of female aggression and its effects.

As being the president of the game company, I urge, insist and command to the distributer not be sell those game's copies. Because business and earning money is not the only factor in your life. If suggested to sell those copies, then it might create the negative impact and consequences in the market and which may ruin the reputation and prestige of the company along with its president and employees. Nowadays even girls play the video games wisely so violating them may lead in economic disturbance to the game company. So rather I would suggest the developer to refine the particular game by not violating the women in any context. This may assist my company's product to flourish more effectively rather than launching it before when it contains the contaminated violation regarding women. Finally, be able to earn more wealth and fame.

Q.6. A Dutch hacker who copied patient files from a University of Washington medical center (and was not caught) said in an online interview that he did it to publicize the system's vulnerability, not to use the information. He disclosed portions of the files (to an individual, not the public) after the medical center said that no patient files had been copied. Was this honorable whistleblowing? (15 marks)

Answer:

This question presents some of the ethical, legal and professional issues invoked by computer hacking. Hacking has been very common to the people. Now it is in big trend. Hacking are also of two categories: one is legal and another one is illegal hacking. Similar to hacking there exist a scenario that a Dutch hacker copied patient's files from a University of Washington medical center and was not caught. He said that he did it to expose system's vulnerability.

I find this not an honorable whistleblowing. As per the medical center is concerned. It is a reputed medical center. It has its own prestige. He must consult to the respective personality of the medical center before disclosing the scenario. If you find anything wrong in the center, then the next step is you must pay attention of the higher authorities towards this case. After the hacker discusses with the concerned body, the decision must be made. If they decide to solve this problem inside their medical center, then hacker must not disclose their patient files but if are discussing unnecessarily and not cooperating with the hacker then further legal attack can be made by the hacker. But directly disclosing the matter might not be the perfect solution for this case. He explains that, he only disclosed to the individual not the public but it's the individual who transfer and communicates to the public people. If an individual gets such information about the medical center than they spread such information rapidly to the public. So it does not make any differences of disclosing it to either individual or public. The result of each scenario is ruining the reputation of the medical center and its employees. The hacker's decision might be considered correct if the concerned authority is not agreeing and paying attention towards your words. But since the concerned center can also sometime unknowingly might make mistakes so they must get the chance to recover their mistakes. Since hacking also

includes sudden principles, ethics and guidelines which must be followed by them. So the perfect response of the hacker to this scenario must be enhancing towards paying attention of the concerned authority rather exposing the system's vulnerability.

Week - 6

Q.1. What does the terms personal information, secondary use and re-identification mean? Give an example for each. (6 marks)

Answer:

Personal information can be almost any information that is associated with an identifiable living individual. Personal information is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Some examples of the personal information include:

→a person's name, address, phone number or email address

→a photograph of a person

→a person's salary, bank account or financial details

→details about a person's land ownership or disputes to do with their land

→details about a person's educational background

→a person's medical details or health information

→a person's fingerprints or blood type

Secondary use makes me think about people lying to get information for other means. It is defined as the use of personal information for a purpose other than the one for which it was supplied. This is a type of exploitation and an invasion of one's privacy.

Some examples of secondary use include consumer information being sold to marketers to use for various reason running schemes on people. Another example would be the use of information in various databases to deny someone a job or to tailor a political pitch. Information like this is used as secondary information to give employers the information they need to know whether they want to hire you for the job or if they do not

want to hire you for the job. People have little control over the secondary uses of their personal data.

Re-identification mean refers in identifying the individual from a set of anonymous data. It is the process by which anonymous personal information is matched with its true owner. In order to protect the privacy interests of consumers, personal identifiers, such as name and social security number, are often removed from databases containing sensitive information. This anonymous information safeguards the privacy of consumers while still making useful information available to marketers or data mining companies.

An example of re-identification would be posting something on the Internet as anonymous and then having it retrace back to you by the IP address on your computer. Re-identification means identifying the individual from a set of anonymous data. Researchers identify people by their monetary value, the vehicles they own, and the sport teams they follow. Once identified, a person is linked to them with the same characteristics. An example is if I search for things on EBay, that information goes into a database on the internet of things I searched and can be linked to other accounts or logins that I have. Law enforcement also uses this tactic to spy on potential predators and threats to our country. Keywords are searched for just like anything else. Findings that are suspicious are immediately red-flagged and reported to the proper authorities.

Q.2. Research Edward Snowden who is currently living in Russia but is wanted by the USA. There is a recent link to content provided by the BBC (British Broadcasting Corporation) relating to Edward in the week 1 content folder. He is likely to provide an interesting topic for much discussion and debate for the duration of this module. Also look up the NSA and GCHQ (Government Communications Headquarters) which have been rather put out by Edward Snowden. Why?

Answer:

Edward Joseph Snowden was born on June 21,1983, is the world's most popular American whistleblower who copied and leaked highly classified information from the National Security Agency (NSA) in 2013 when he was as a Central Intelligence Agency (CIA) employee and a subcontractor. The famous whistleblower had revealed how US secretly collects the private data from the renowned companies like; Facebook, Google, Microsoft, Yahoo, YouTube, Skype, Apple and Pal talk (the largest video chat room community) in the Guardian newspaper. The documents revealed the scale of mass surveillance by the US, UK and their allies (supporters). He is on the US most wanted list. Previously who used to dislike him are now his supporters. He explains that Russia glanced him as an essential publicity. Since Russia and US were the great fortress of the enemy which is the way a CIA agent looks at Russia so it was hard for Snowden to openly speak about Russia. It was hard for Edward because if he spoke about Russia it would be difficult for him back home i.e. US. Edward has been guaranteed asylum and has apparently found a new job in Russia. He is now working in technical support on a major Russian website.

Snowden explained that he viewed himself as a patriot, believing his actions had beneficial results. He stated that his leaking of information led to "a robust (tough or powerful) public debate" and "new protections in the United States and abroad for our rights to make sure they're no longer violated." He also expressed an interest in returning home to America. But according to the US he was soon charged with the statement "theft of the government property", "unauthorized communication of national defense

information" and "willful communication of classified communications intelligence information to an unauthorized person".

Q.3. Life insurance companies are experimenting with analysis of consumer profiles (to determine whether a person eats healthy food, exercises, smokes or drinks too much, has high-risk hobbies, and so on) to estimate life expectancy. Companies might use the analysis to find populations to market their insurance policies to. From the perspective of privacy, what are some of the key ethical or social issues raised? Evaluate some of them. (15 marks)

Answer:

The premium rate for a life insurance policy is also based on life expectancy (or mortality rate). Life insurance is based on the sharing of the risk of death by a large group of people. The amount at risk must be known to predict the cost to each member of the group. Mortality tables are used to give the company a basic estimate of how much money it will need to pay for death claims each year. By using a mortality table, a life insurer can determine the average life expectancy for each age group.

Life expectancy is the foremost factor in determining an individual's risk factor and the likelihood they will make a claim. Insurance companies consider age, lifestyle choices (comprises of food, health, hobbies and so on), family medical history and other several related factors when determining a premium rate for individual life insurance policies. There exhibits a direct correlation between your life expectancy and how much you will be charge for a life insurance policy. The younger you are when you purchase a life insurance policy, the longer you are likely to live which means that there is a lower risk to the life insurance company because you are less likely to die which ultimately lead full benefit of your policy before you have paid much into the policy. Conversely, the longer you wait to purchase life insurance, the lower your life expectancy, and that translates into a higher risk for the life insurance company. Companies compensate for that risk by charging a higher premium. Since for their companies benefit the company target your profiles and lifestyle to know if he/she can benefit our company or not by performing insurance policy. As older and unhealthy you become there is more possibility of you dying which can harm the company so they do not market for such areas. On the other

hand, if there are young faces who are even healthy then they are urged to do insurance policy so that they can profit their company. So knowing the consumers profile can assist the insurance company in marketing.

Q.4. A company in the Netherlands that makes navigation devices collects location data from the devices to provide real-time services to its customers. It also provides anonymous statistical data to government agencies to improve roads and traffic flow. Unknown to the company and its customers, the police used the data to choose sites for traffic cameras to catch speeders. Was this a privacy violation? Why or why not? (10 marks)

Answer:

The reasonable advantage of the navigation devices is to give geographical information and traffic density of zones as statistical information. But in Netherland the data captured by the navigation devices has been purchased by the country's police force and is being used to determine where speed traps and cameras should be placed. The company was unaware that its data were being used in such a way. It is definitely the privacy and policy violation. The company provides the effective help to the customers but the data collected by the traffic violets the privacy.

The company primarily ask for your permission to collect those data. They try to make all the traffic data anonymous so that tracing it back cannot be possible. They assist in providing us the fastest route by turning anonymous data into traffic information which ultimately can help make roads flow more effective, efficient and safer. The major goal of such company is to create driver and rider community capable of reducing traffic jams and congestion (overcrowding) for everybody. But the problem is in police force, they try to purchase such data and information for their benefit. They purchase the location or navigation data and use them for tracing these customers and finally use these data to choose sites for the traffic cameras and to catch speeders. The initiative of catching the speeders is good because lot of accidents are caused due to over speeding bit the way of doing this is not meant to be good. Tracing the customers by their statistical data without the permission is not meant to be right. The sensitive information of the customers is also being expose to those police department which is illegal. Using such information,

they ca go personal with whoever they want. Misuse of the information can be common. So we can sum up that they are clearly violating the privacy. To ensure the safety of these privacy the companies are making the data anonymous. After this all this data is being collected anonymously and the police have no idea exactly who is speeding, just that speeding has occurred.

Q.5. A company planned to sell a laser device a person can wear around his or her neck that makes photographs taken of the person come out streaked and useless. The company marketed it to celebrities hounded by photographers. Suppose the device works well against surveillance cameras commonly used in public places and in many businesses. Many people begin to use the device routinely when outside their homes. But the law enforcement agencies propose making its use illegal. Give arguments for and against such a proposal. (15 marks)

Answer:

As celebrities are anytime crowded by their fans and photographers, which makes them feel unsafe and uncomfortable. As a result, they try to hide and be away from them although they love such craze and fan love but they are compelled to do so. So for safeness and comfortableness purpose of the celebrities a device called laser device is available in market for them. These devices are for the celebrates who are hounded by enormous photographers. Laser device works well against surveillance cameras that are commonly applied in public places and businesses. These devices might be required to them for maintaining their privacy as well.

But on the other hand if they are allowed to use such technology (laser device), then not all but some may misuse it as well. They can use it wherever, whenever and however they desire. They can apply it in daily routine basis which may be illegal (against the law). Since they accurately and effectively work against the surveillance cameras so they can do mischievous kind of activities in the public places and ca easily get rid of by the assist of this technology. So every task and subject contains it's both bright and dark side. For that bright sides should be formulated and dark side must be left out. For only implementing the bright side, strict law must be enforced and enhanced by the government towards such celebrities as per they are using such laser devices for their security and privacy purposes.