**Handouts of Lecture 8 Professional Practices (IT)**

**Lecture Title: Networking (Cont)**

**Children and Inappropriate Content**

Many parents and guardians believe they ought to protect their children from exposure to pornographic and violent materials. A few years ago the center of concern was the Web, and a large software industry sprang up to provide browsers with the ability to block inappropriate images. Now smartphones are becoming commonplace, and some parents are being forced to confront the unpleasant reality that their children have emailed sexually provocative images of themselves to friends or even strangers.

**Web filter** is a piece of software that prevents certain Web pages from being displayed by your browser. While you are running your browser, the filter runs as a background process, checking every page your browser attempts to load. If the filter determines that the page is objectionable, it prevents the browser from displaying it. Typical filters use two different methods to determine if a page should be blocked. The first method is to check the URL of the page against a blacklist of objectionable sites. If the Web page comes from a blacklisted site, it is not displayed. The second method is to look for combinations of letters or words that may indicate a site has objectionable content. Neither of these methods is foolproof. The Web contains millions of pages containing pornography, and new sites continue to be created at a high rate, so any blacklist of pornographic sites will be incomplete by definition. Some filters sponsored by conservative groups have blacklisted sites associated with liberal political causes, such as those sponsored by the National Organization for Women and gay and lesbian groups. The algorithms used to identify objectionable words and phrases can cause Web filters to block out legitimate Web pages.

**Child Internet Protection Act**

In March 2003, the Supreme Court weighed testimony in the case of United States v. American Library Association. The question: Can the government require libraries to install antipornographic filters in return for receiving federal funds for Internet access? More than 14 million people access the Internet through public library computers. About one-sixth of the libraries in the United States have already installed filtering software on at least some of their computers. The Child Internet Protection Act requires that libraries receiving federal funds to provide Internet access to its patrons must prevent children from getting access to visual depictions of obscenity and child pornography. The law allows adults who desire access to a blocked page to ask a librarian to remove the filter. In his testimony before the Supreme Court, Solicitor General Theodore Olson argued that since libraries don’t offer patrons X-rated magazines or movies, they should not be obliged to give them access to pornography over the Internet.

**Ethical evaluation of CIPA**

**Kantian evaluation**: The goal of CIPA is to protect children from the harm caused by exposure to pornography. The way the goal is being implemented is through Web filters. Studies have demonstrated that Web filters do not block all pornographic material but do block some nonpornographic Web pages. Some nonpornographic information posted on the Web is not easily accessible at libraries implementing government-mandated Web filters. The people posting this information did not consent to their ideas being blocked. Hence the decision to require the use of Web filters treats the creators of non-offensive but blocked Web pages solely as means to the end of restricting children’s access to pornographic materials. This analysis leads us to conclude that CIPA is wrong.

**Act utilitarian evaluation**: Second evaluation of CIPA is from an act utilitarian point of view. What are the consequences of passing CIPA?

1. While not all children access the Web in public libraries, and while Web filtering software is imperfect, it is probable that enacting CIPA results in fewer children being exposed to pornography, which is good.

2. Because Web filters are imperfect, people are unable to access some legitimate Web sites. As a result, Web browsers in libraries are less useful as research tools, a harmful consequence.

3. Adult patrons who ask for filters to be removed may be stigmatized (rightfully or not) as people who want to view pornography, a harm to them.

4. Some blocked sites may be associated with minority political views, reducing freedom of thought and expression, which is harmful.

Whenever we perform the utilitarian calculus and find some benefits and some harms, we must decide how to weigh them. This is a good time to think about utilitarian philosopher Jeremy Bentham’s seven attributes. In particular, how many people are in each affected group? What is the probability the good or bad event will actually happen? How soon is the event likely to occur? How intense will the experience be? To what extent is the pain not diluted by pleasure or vice versa? How long will it last? How likely is the experience to lead to a similar experience? Actually performing the calculus for CIPA is up to each person’s judgment. Different people could reach opposite conclusions about whether enacting CIPA is the right thing for the US government to do.

In **Social contract theory**, morally binding rules are those rules mutually agreed to in order to allow social living. Freedom of thought and expression is prized. According to John Rawls, “liberty of conscience is to be limited only when there is a reasonable expectation that not doing so will damage the public order which the government should maintain”. Some argue that allowing people to view pornography in a public place demeans women, denying them dignity as equal persons. On the other hand, we know that filtering software is imperfect. In the past it has been used to promote a conservative political agenda by blocking sites associated with other viewpoints. Hence it reduces the free exchange of ideas, limiting the freedoms of thought and expression. For some adults, public libraries represent their only opportunity to access the Web for no cost. In order to be treated as free and equal citizens, they should have the same Web access as people who have Internet access from their homes. If Web filters are in place, their access is not equal because they must ask for permission to have the filters disabled. Finally, while most people would agree that children should not be exposed to pornographic material, it would be harder to convince reasonable people that social living would no longer be possible if children happened to see pornography in a library. Our analysis from the point of view of social contract theory has produced arguments both supporting and opposing the Children’s Internet Protection Act. However, installing filters does not seem to be necessary to preserve the public order. For this reason, the issue is outside the social contract and freedom of conscience should be given precedence.

**Sexting**

Sexting refers to sending sexually suggestive text messages or emails containing nude or nearly nude photographs. In a 2009 survey of 655 American teenagers conducted by Cox Communications, 9 percent said they had sent a sext at least once, 17 percent said they had received a sext at least once, and 3 percent said they had forwarded a sext at least once. Of the teens who had sent sexts, 11 percent admitted to having sent a sext to someone they didn’t know

Although sexting is a relatively recent phenomenon, there are already plenty of stories in the mainstream media about the serious impact it is having on people’s lives.

**Breaking Trust**

**Identity Theft**

Dorothy Denning defines identity theft as “the misuse of another person’s identity, such as name, Social Security number, driver’s license, credit card numbers, and bank account numbers. The objective is to take actions permitted to the owner of the identity, such as withdraw funds, transfer money, charge purchases, and get access to information, or issue documents and letters under the victim’s identity”. The leading form of identity theft in the United States is credit card fraud. Identity thieves either take out a new credit card in someone else’s name or commandeer an existing account. By changing the billing address of existing accounts, a thief can run up large debts before the victim becomes aware of the problem. These activities can blemish the target’s credit history. As a result, victims of identity theft may have applications for credit cards, mortgage loans, and even employment denied. If the impostor shows false credentials to the police, the victim may even be saddled with a false criminal record or outstanding arrest warrants. Financial institutions contribute to the problem of identity theft by making it easy for people to open up new accounts. Since information brokers on the Web are selling driver’s license numbers, Social Security numbers, and credit card information, it’s easy for an identity thief to gather a great deal of information about another person. Assuming another person’s identity is made simpler by banks allowing people to open accounts online.

Surprisingly, 14 percent of the cases of identity theft identified in 2010 were “friendly thefts” in which family members, friends, or in-house employees made purchases without the account holder’s consent. Still, a significant number of people are victims of identity theft through their online activities. Gathering financial information via spam is called phishing (pronounced “fishing”). Thieves send out spam messages designed to look like they originated from PayPal, eBay, or another well-known Internet-active business. Through these messages they hope to con unsuspecting recipients into connecting with authentic-looking Web sites and revealing their credit card numbers or other personal information. For example, a victim might receive an email message purportedly from PayPal, asking the person to go to the PayPal Web site to confirm a transaction. The email message contains a hypertext link. When the victim clicks on the link, he is connected to the counterfeit PayPal site. Phishing, spyware, and other online methods resulted in more than a million cases of identity theft in the United States in 2008.

**Chat Room Predators**

Instant messaging is a real-time communication between two or more people supported by computers and a telecommunications system. A chat room is similar to instant messaging, except that it supports discussions among many people. A large number of organizations sponsor chat rooms dedicated to a wide variety of topics. For example, in July 2009, America Online’s “Chats” page listed hundreds of chat rooms divided into 30 general categories, including Arts and Entertainment, Black Voices, Friends & Flirts, GLBT, Latino, Life, Places, Politics, Romance, and Town Square. The popularity of instant messaging varies from country to country. According to Nielsen/NetRatings, the number of people who used instant messaging between January and March of 2002 varied from 13 percent of all Internet users in Denmark to 43 percent in Spain. Participation in chat rooms also varies from country to country. According to the same survey, the number of people with Internet accounts who participated in a chat room between January and March of 2002 varied from 16 percent in the United Kingdom to 41 percent in Brazil. In 1999 the FBI investigated 1,500 crimes in which an alleged pedophile crossed a state line to meet and molest a child met through an Internet chat room. Many say the problem is growing. Parry Aftab, executive director of Cyber Angels, says, “I know that I can go into a chat room as a 12-year-old and not say anything, and be hit on and asked if I’m a virgin within two minutes”. Police have begun entering chat rooms posing as young girls to lure pedophiles. During a three-week-long sting operation in Spokane, Washington, a police detective posed as a 13-year-old girl in a chat room. In early March 2003, police arrested a 22- year-old man on charges of attempted second-degree rape of a child. Inside his car the officers found handcuffs, a large folding knife, and a condom. The suspect was still on parole for an earlier conviction for fourth-degree assault with sexual motivation. Police sergeant Joe Petersen asked, “What happens had it been a real girl?” Chat-room sting operations are leading to many arrests all over the United States.

**Ethical Evaluation of Sting operation**

**Utilitarian analysis**. Let’s consider the various consequences of such a sting operation. A person allegedly interested in having sex with an underage minor is arrested and charged with attempted child rape. Suppose the person is found guilty and must serve time in prison. The direct effects of the sting operation are the denial of one person’s freedom (a harm) and an increase in public safety (a benefit). Since the entire public is safer and only a single person is harmed, this is a net good. The sting operation also has indirect effects. Publicity about the sting operation may deter other chat-room pedophiles. This, too, is a beneficial result. It is harder to gauge how knowledge of sting operations influences innocent citizens. First, it may reduce citizens’ trust in the police. Many people believe that if they are doing nothing wrong, they have nothing to fear. Others may become less inclined to provide information to the police when requested. Second, sting operations can affect everyone’s chat-room experiences. They demonstrate that people are not always who they claim to be. This knowledge may make people less vulnerable to being taken advantage of, but it may also reduce the amount of trust people have in others. Sting operations prove that supposedly private chat-room conversations can actually be made public. If chat-room conversations lack honesty and privacy, people will be less willing to engage in serious conversations. As a result, chat rooms lose some of their utility as communication devices. How much weight you give to the various consequences of police sting operations in chat rooms determines whether the net consequences are positive or negative.

**Kantian analysis**: A Kantian focuses on the will leading to the action rather than the results of the action. The police are responsible for maintaining public safety. Pedophiles endanger innocent children. Therefore, it is the duty of police to try to prevent pedophiles from accomplishing what they intend to do. The will of the police detective is to put a pedophile in prison. This seems straightforward enough. If we dig a level deeper, however, we run into trouble. In order to put a pedophile in prison, the police must identify this person. Since a pedophile is unlikely to confess on the spot if asked a question by a police officer, the police lay a trap. In other words, the will of the police detective is to deceive a pedophile in order to catch him. To a Kantian, lying is wrong, no matter how noble the objective. By collecting evidence of chat-room conversations, the police detective also violates the presumed privacy of chat rooms. These actions of the police detective affect not only the alleged pedophile but also every innocent person in the chat room. In other words, detectives are using every chatroom occupant as a means to their end of identifying and arresting the pedophile. While police officers have a duty to protect the public safety, it is wrong for them to break other moral laws in order to accomplish this purpose. From a Kantian point of view, the sting operation is morally wrong.

**Social contract theory analysis**: An adherent of social contract theory could argue that in order to benefit everyone, there are certain moral rules that people in chat rooms ought to follow. For example, people ought to be honest, and conversations ought to be kept confidential. By misrepresenting identity and/or intentions, the pedophile has broken a moral rule and ought to be punished. In conducting sting operations, however, police detectives also misrepresent their identities and record everything typed by suspected pedophiles. The upholders of the law have broken the rules, too. Furthermore, we have the presumption of innocence until proof of guilt. What if the police detective, through miscommunication or bad judgment, actually entraps someone who is not a pedophile? In this case, the innocent chat-room users have not broken any rules. They were simply in the wrong place at the wrong time. Yet society, represented by the police detective, did not provide the benefits chat-room users expect to receive (honest communications and privacy). In short, there is a conflict between society’s need to punish a wrongdoer and its expectation that everyone (including the agents of the government) abide by its moral rules.

**False operation**

The Web is a more open communication medium than newspapers, radio stations, or television stations. Individuals or groups whose points of view may never be published in a newspaper or broadcast on a television or radio show may create an attractive Web site. The ease with which people may get information out via the Web is one of the reasons the Web contains billions of pages. However, the fact that no one has to review a Web page before it is published means the quality of information available on the Web varies widely.

In traditional publishing, various mechanisms are put in place to improve the quality of the final product. For example, before Addison-Wesley published the first edition of this book, an editor sent draft copies of the manuscript to a dozen reviewers who checked it for errors, omissions, or misleading statements. The author revised the manuscript to respond to the reviewers’ suggestions. After the author submitted a revised manuscript, a copy editor made final changes to improve the readability of the text, and a proofreader corrected typographical errors. Web pages, on the other hand, can be published without any review. As you’re undoubtedly well aware, the quality of Web pages varies dramatically. Fortunately, search engines can help people identify those Web pages that are most relevant and of the highest quality. Let’s take a look at how the Google search engine does this.

The Google search engine keeps a database of many billions of Web pages. A software algorithm ranks the quality of these pages. The algorithm invokes a kind of voting mechanism. If Web page A links to Web page B, then page B gets a vote. However, all votes do not have the same weight. If Web page A is itself getting a lot of votes, then page A’s link to page B gives its vote more weight than a link to B from an unpopular page. When a user makes a query to Google, the search engine first finds the pages that closely match the query. It then considers their quality (as measured by the voting algorithm) to determine how to rank the relevant pages.

**Cyberbullying**

Cyberbullying is the use of the Internet or the phone system to inflict psychological harm on another person. Frequently, a group of persons gangs up to cyberbully the victim. Examples of cyberbullying include. Repeatedly texting or emailing hurtful messages to another person. Spreading lies about another person. Tricking someone into revealing highly personal information. “Outing” or revealing someone’s secrets online. Posting embarrassing photographs or videos of other people without their consent. Impersonating someone else online in order to damage that person’s reputation. Threatening or creating significant fear in another person Surveys have revealed that cyberbullying is common among teenagers. Cox Communications surveyed 655 American teenagers in 2009, and 19 percent reported that they had been cyberbullied online, via cell phone, or through both media. Ten percent of the teenagers admitted to cyberbullying someone else. When asked why they had cyberbullied someone else, the most common responses were “they deserved it” and “to get back at someone.

In some instances cyberbullying has led to the suicide of the victim, as in the case of 13-year-old Megan Meier. According to her mother, “Megan had a lifelong struggle with weight and self-esteem”. She had talked about suicide in third grade, and ever since then she had been seeing a therapist. Megan’s spirits soared when she met a 16-year-old boy named Josh Evans on MySpace. They flirted online for four weeks but never met in person. Then Josh seemed to sour on their relationship. One day he let her know that he didn’t know if he wanted to be friends with her anymore. The next day he posted: You are a bad person and everybody hates you. Have a shitty rest of your life. The world would be a better place without you. When Megan angrily responded to this post, others ganged up on her: “Megan Meier is a slut”; “Megan Meier is fat”. Later that afternoon, Megan hanged herself in her bedroom. Eventually the community learned that “Josh Evans” did not exist. The MySpace account had been created just a couple of houses away from the Meier home by 18-yearold Ashley Grills, 13-year-old Sarah Drew, and Lori Drew, Sarah’s mother. Sarah had a falling out with Megan, and Ashley suggested creating the MySpace account to find out what Megan might be saying about Sarah. Lori Drew had approved the plan. Most of the messages from “Josh” had been written by Sarah or Ashley, but Lori Drew had been aware of what they were doing. The county’s district attorney declined to prosecute Lori Drew because there was no Missouri law against cyberbullying. The FBI investigated the case, however, and in 2008 federal prosecutors charged Drew with four felony counts under the Computer Fraud and Abuse Act for violating the MySpace terms of service. A jury found her not guilty of these crimes but did convict her of three misdemeanors. In 2009 a US district judge overturned these convictions, stating that criminal charges should not have been brought against Drew for breaking a contract with an Internet service provider. In April 2009, the Megan Meier Cyberbullying Prevention Act was introduced in the US House of Representatives. The purpose of the proposed law was to “impose criminal penalties on anyone who transmits in interstate or foreign commerce a communication intended to coerce, intimidate, harass, or cause substantial emotional distress to another person, using electronic means to support severe, repeated, and hostile behavior”.

**Internet Addiction**

The traditional definition of addiction is the persistent, compulsive use of a chemical substance, or drug, despite knowledge of its harmful long-term consequences. Some people spend between 40 and 80 hours per week on the Internet, with individual sessions lasting up to 20 hours. Spending so much time online can have a wide variety of harmful consequences. Fatigue from sleep deprivation can lead to unsatisfactory performance at school or at work. Physical ailments include carpal tunnel syndrome, back strain, and eyestrain. Too many hours in front of a computer can weaken or destroy relationships with friends and family members. In a few cases, people have died after prolonged sessions sitting in front of a computer. Kimberly Young created a test for Internet addiction. Using the diagnosis of pathological gambling in the Diagnostic and Statistical Manual of Mental Disorders as her starting point, Young produced an eight-question screening instrument that probes how Internet usage is affecting the patient’s life, including how preoccupied the patient is with the Internet, whether the patient has been repeatedly unsuccessful in reducing Internet usage, and how the patient feels when trying to spend less time online. According to Young, patients who answer yes to five or more of these questions appear to be addicted to the Internet, unless “their behavior could not be better accounted for by a Manic Episode”. Young’s use of the phrase “Internet addiction” and her questionnaire are controversial. John Charlton points out that computer use, unlike drug use, is generally considered to be a positive activity. In addition, while drug addiction leads to an increase in criminal activity, the same level of societal harm is unlikely to occur even if the Internet is overused by some people. Charlton performed his own study of computer users and has concluded that Young’s checklist approach is likely to overestimate the number of people addicted to the Internet. According to Charlton, some “people who are classified as computer-dependent or computer-addicted might often be more accurately said to be highly computer-engaged”.

**Contributing factors**

According to Peele, social, situational, and individual factors can increase a person’s susceptibility to addiction. For example, peer groups play an important role in determining how individuals use alcohol and other drugs. People in stressful situations are more likely to become addicted, as are those who lack social support and intimacy, and those who have limited opportunities for “rewarding, productive activity”. Individual factors that make a person more susceptible to addiction include a tendency to pursue an activity to excess, a lack of achievement, a fear of failure, and feelings of alienation. Young’s studies have led her to “believe that behaviors related to the Internet have the same ability to provide emotional relief, mental escape, and ways to avoid problems as do alcohol, drugs, food, or gambling”. She notes that the typical Internet addict is addicted to a single application.

**Ethical Evaluation**

People who use the Internet excessively can harm themselves and others for whom they are responsible. For this reason, excessive Internet use is a moral issue. Kantianism, utilitarianism, and social contract theory all share the ***Enlightenment view*** that individuals, as rational beings, have the capacity and the obligation to use their critical judgment to govern their lives. Kant held that addiction is a vice, because it’s wrong to allow your bodily desires to dominate your mind. Mill maintained that some pleasures are more valuable than others and that people have the obligation to help each other distinguish better pleasures from worse ones. Ultimately, people are responsible for the choices they make. Even if an addict is “hooked,” the addict is responsible for choosing to engage in the activity the first time. This view assumes that people are capable of controlling their compulsions. According to Jeffrey Reiman, vices are “dispositions that undermine the sovereignty of practical reason. Dispositions, like habits, are hard but not impossible to overcome, and undermining something weakens it without necessarily destroying it entirely”.

***Riemann’s view*** is supported by Peele, who believes addicts can choose to recover from their addictions. “People recover to the extent that they (1) believe an addiction is hurting them and wish to overcome it, (2) feel enough efficacy to manage their withdrawal and life without the addiction, and (3) find sufficient alternative rewards to make life without the addiction worthwhile”.

***Reference:***

***Lecture topic: Networking slides***

***Gao, Y. (2012). Ethics for the Information Age by Michael J. Quinn. World Libraries, 20(1).***