Jacob Davies

Professor Henderson

CSCI 325

21 June 2018

Ethics Paper

Ethical issues are not just black and white. While some may be simple to determine what is right and wrong, like stealing from someone. Other ethical issues may not be as simple. For example, if storing records of what the users of a website are searching for is unethical because it invades their privacy or if it helps the website better cater to its users. In this situation it is important to look to the bible and other ethical resources to determine the course of action. There are many different ethical issues within the realm of computer science, so I will cover 3 different kinds: computer crime, privacy of users, and protection of software rights.

One of the most clear-cut ethical issues within computer science is computer crime. This includes activities such as: identity theft, stealing money from computer systems, sabotaging systems via viruses, etc. It is clear-cut in the sense that it is obvious that these activities are wrong and should be punished, as the bible tells us, “You shall not steal.” (*The Holy Bible.* ESV, Exodus 20:15). However, defending against computer crimes can be quite complex and even involves the entire field of ethical hacking to help prevent crime. Although this type of crime is wrong it is not always punished adequately, “Often the worst that can happen to such a thief is that he/she is merely required to return the stolen money. Many times that person will be fired, assuming he/she is an employee, but may be quickly hired by a competitor because of his/her skill.” (Berzai). To handle cybercrime, it is important that ethical hacking and penetration testing is still practiced and carried out in the workplace.

Privacy issues are more ambiguous in terms of their ethical determination. This is because whenever you collect data or a record of a user’s actions it can be used to better whatever software is being used, but if the software happens to be hacked then the hacker would have access to any personal information the software recorded from the user which puts the user at risk. I think that because there is potential for both good and bad when it comes to privacy issues there should be a balance of what is stored and what is not. I suggest that companies use a risk-reward system where they consider if a hacker accessed this information what damage could they do versus what good could the company do to better their software based on the information. This way they can narrow down what information about their users they store in a logical manner that also follows the first two general moral imperatives from the AMC Code of Ethics and Professional Conduct; 1.1 Contribute to society and human well-being, and 1.2 Avoid harm to others.

Protection of software rights means making sure people do not take credit for the work of others in a computer science setting. This is important because it is only fair for the group of people or person who made the program to receive the credit for their work. Sometimes it may be tricky to develop your own applications without looking at other people’s projects in order to generate ideas of your own. If this is the case a good solution would be to give credit to other projects that were responsible for helping you in your endeavors. A verse that is a great reminder when it comes to protecting software rights says, “And as you wish that others would do to you, do so to them.” (*The Holy Bible.* ESV, Luke 6:31).

Works Cited

ACM council. “ACM Code of Ethics and Professional Conduct.” www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct#sect1. Accessed June 22, 2018.

Berzai, Lou. “Ethical Problems in Computing.” Aitp.org. www.aitp.org/blog/aitp-blog/2017/07/04/ethical-problems-in-computing/. Accessed June 22, 2018.

*The Holy Bible.* English Standard Version, Crossway, 2001.