

Alex Thompson

Prof. Henderson

CSCI 325

6 November 2021

The Ethical Responsibilities of a Professional

In many different career paths, ethics is a huge part in developing a product or service that helps others to make their lives easier. In my career path, computer science, there are many different ethical dilemmas that programmers and others in the field come across, and the range of these dilemmas are quite large. There are many challenges that programmers need to overcome and find out ways to solve these issues with in an ethically correct way. The main ethical dilemma I will personally face at work as a professional in my chosen field is easily the ethics of privacy and safety while handling the private information of users, as the users expect their private information to be safe while using a program or website that is developed, and to make sure all of the user's information is safe is a very important job for many professionals inside my chosen field.

I believe that the biggest ethical dilemma in my professional field that I will face is the safety and privacy of the users, along with their private information and how that information is used for the program or site. With constant hacks and data leaks from websites and applications, the importance of keeping this information secured is very important, as almost all users do not want their information roaming around the internet. For every single website, the "security and privacy" of users that the users enter is "rarely end-users' primary tasks", and the "users have limited mental resources" about where their information is stored, how the information is used, and who is able to see their information, so if anything happens to the information, the users will

not be able to see the “consequences of their actions” (Acquisti 2). The users not being able to see what their data is being used for and trusting the site or application to use the data in ethical ways is one of the biggest dilemmas when it comes to the internet and its safety, which is similar to the IEE Code of Ethics principle 2, which describes how in the field, people should help improve the understanding of these technologies and what their data is being used for. Users are often worried about “security threats like eavesdropping and denial of services” that a programmer’s application or site can possibly have, which are very reasonable worries to have due to many sites using these methods to garner information to help advertising and provide recommendations based on the user’s likings (Al Ameen). I personally would not want to use methods that can trespasses people’s privacy, like eavesdropping, but this is a practice that is seen in my field, as the trust of users using the program or site is more important, and the use of this practice to harvest information is not ethically correct. Leading from companies gathering information, “privacy issues in the Internet age have received significant attention” overtime due to the discovery of these companies using unethical methods to gather information, but mainly the “allegations of governments spying on their citizens” through the data the users provide on the internet has people terrified (Perera 33). The concern of the users using one of my programs over the safety of their private information is easily one of the biggest ethical dilemmas I will have to face in my profession, as with more and more companies being caught doing unethical methods to harvest and sell information, like how Facebook was caught in 2019, to gain the trust of the users is very important for the success of a developer.

I propose that in order for one to prepare to handle or overcome these dilemmas is to be very open and clear to your users about what information and data is being collected and what is happening with the data, even outside of the terms and conditions. A great way to gain the trust

of users is to open-source applications that you have created, as users who are curious enough to dig through and see the code of a program can discover that the information being gathered is not being used for malicious or unethical purposes, which helps show principle 1.3 of the ACM Code of Ethics, which says to be honest and trustworthy, which to open-source the application means to show the program is not hiding anything malicious and does not need to hide from the public. I personally do not feel as prepared for these challenges, as there has been many situations where hackers break into the system and steal information or massive data leaks happen, and the person responsible is the person who developed the security measures to make sure the data is secured, and even if I am not the person who coded the security, knowing that a program or site you developed is responsible for tons of trusted user's information being leaked to the public is very scary and a huge responsibility. Companies take the course of action to hide all their code, and even trying to sue people who try to reverse-engineer said code for their own programs, all in order to protect their code, but that only creates more suspicion on what the company is doing with the peoples' information, which is not ethically correct. The specific actions I would take to be prepared is to make sure that the security and encryption of the private information of users is extremely secure, and make sure the personal information is secure before a release.

The ACM Code of Ethics and Professional Conduct and the IEEE Code of Ethics show the many ethical aspects of working in a professional environment that should be respected and shown by all people working. Many of these ethical principles can be compared to certain Biblical principles that show how to live life and treat the others around each other. An example of the principles from the ACM Code of Ethics and Professional Conduct is principle 3.1, which states that the public good is the main concern of all professional work, which if you compare the

Biblical principle of Titus 2:7-8, the verse states that a person should always set an example by doing good, which helps to teach integrity as if you do good, there will be nothing bad to say. These two principles compare as setting a good example for the public good will help make the company you work for be trusted and reach a level where the reputation will carry the product, as people can only say good about a person's work. An example of the principles from the IEEE Code of Ethics is principle 6, which states that in order to maintain and improve a business, tasks must only be taken by qualified professionals, which must disclose their limitations. The comparison of that principle to the Biblical principle of 2 Thessalonians 3:10, which states that if a person is not willing to work, they shall not be fed, shows that if a person is not hard working and does not forward the progress of society or the company, they should not be rewarded as much compared to someone who works hard as professional. Overall, the ACM Code of Ethics and Professional Conduct and the IEE Code of Ethics both show the many ethics professionals should follow in the workplace, especially when creating a product or service, which is very comparable to Biblical principles that people follow and live by during their life.

No matter what profession a person chooses, a professional in any field and business must follow the different codes of ethics in order to present a reputation for the public and the people around them. To follow these principles like Biblical principles helps create a more trustworthy environment to work in, especially if you apply both principles to the people around you and in the work place. With all of the possible dilemmas that can appear in my chosen profession of computer science, I will follow these codes of ethics and implement them into my daily life and in anything I create, as doing so helps create a more professional and respectful work environment for everyone around.

Works Cited

- Acquisti, Alessandro, et al. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." *ACM Computing Surveys*, vol. 50, no. 3, ACM, 2017, pp. 1–41, doi:10.1145/3054926.
- Al Ameen, Moshaddique, et al. "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications." *Journal of Medical Systems*, vol. 36, no. 1, Springer US, 2010, pp. 93–101, doi:10.1007/s10916-010-9449-4.
- Perera, Charith, et al. "Big Data Privacy in the Internet of Things Era." *IT Professional*, vol. 17, no. 3, IEEE, 2015, pp. 32–39, doi:10.1109/MITP.2015.34.