

Morals of My Cybersecurity Career, Life, and future

The course "Ethics of Cybersecurity" has been an important learning opportunity for me, and I have gathered a deeper understanding of the ethical issues that can come up in the field of cybersecurity. I have also had the opportunity to consider different perspectives on these issues, and to develop my own ethical framework for cybersecurity as I wrote my papers and thought about why people acted the way they did.

In this reflection, I will discuss three topics, perspectives, or positions that I have found interesting and that have helped me develop my own ethics while working in this course. For each topic, I will write about how my position or how my thoughts have changed, deepened, or gained a different meaning. I will also write down a "takeaway" for each topic in the form of something I would like my future self to remember and be guided by.

Topic 1: Privacy

The concept of privacy has been a hotly debated topic for many years, and it is only becoming more complex as technology advances. In Module 1, we discussed the different ways in which privacy can be defined, and the ethical implications of different approaches to privacy.

I have always considered myself to be a strong supporter for privacy, but my understanding of this concept has deepened as a result of this course. I now have a better understanding of the different ways that a person's privacy can be violated and why privacy is important. I learned about the potential consequences of these violations too. I also have a better understanding of the different things that can influence our privacy expectations, such as our culture, our values, and our technology use.

Takeaway: Privacy is a fundamental human right, and it is important to protect our privacy in the digital world. But, privacy is not an absolute right, and there are some cases where it may be necessary to compromise our privacy in order to accomplish the greater good. It is important to weigh the different influencers involved in each case in order to make the most ethical decision.

Topic 2: Data Ethics

The collection and use of data is becoming increasingly important in the digital world. However, there are a lot of ethical issues that come up when we think of data collection and how it is used. In Module 2, we talked about some of these ethical issues; issues like the right to privacy, the use of personal data for marketing purposes, and the use of big data for social research.

I have always been interested in the potential for data collection and how it is being used for ethical or unethical purposes. I've really gotten in deep with my readings of GDPR due to other classes too. But my understanding of these issues has grown because of this course and its content. I now have a better understanding of the different ways that data can be collected and used, and the potential moral consequences of these uses. I also have a better understanding of the different moral frameworks that can be used to guide data collection and use.

Takeaway: Data is a powerful tool, and it is important to use it ethically. When collecting and using data, it is important to respect the privacy of individuals, and to use the data for legitimate and legal purposes. It is also important to be transparent about how the data is being collected and used before it is ever collected, and to give people the opportunity and right to opt out of data collection.

Topic 3: Whistleblowing

Whistleblowing is the act of reporting unethical or illegal activity to the authorities. In Module 5, we discussed the ethical consequences of whistleblowing, and the different events and influences that can cause a person to make the decision of blowing the whistle.

I have not always been a strong supporter of whistleblowing, I thought it was breaking the law before this course. I thought loyalties lay with the company especially when it came to government but now I believe that it is an important way to hold organizations accountable for their actions and keep our country moral. I have also started to understand that whistleblowing can be a risky course of action though, and that there are a number of possible consequences for whistleblowers.

Takeaway: Whistleblowing is an important tool for holding organizations accountable, but it is also a risky tool. Before blowing the whistle, it is important to carefully consider the potential consequences, and to make sure that you have the support of others and you have exhausted your other possible ways of internal reporting.

These are just three of the many topics that I have learned and grown from through my studying of in this course. I have learned a lot about the ethical issues that can come up in the field of cybersecurity, and I have developed a deeper understanding of the ethical frameworks and morals that can be used to guide cybersecurity practice. I am glad I took this course, and I am confident that the information and skills I have collected will be valuable in my career in cybersecurity.