Reflective Writing Assignment

Throughout PHIL 355, I learned that ethics in technology is not just about knowing what is legal or illegal. It is also about asking what should be done when people, companies, and especially governments have access to powerful tools and large amounts of personal data. As a cybersecurity major, this class helped me see that my future career will involve more than technical skills. I will also have to think about privacy, responsibility, harm, and fairness when dealing with systems that affect real people.

One topic that stood out to me was privacy and user data. Before this course, I mostly thought about privacy from a security perspective, such as protecting passwords, preventing breaches, and stopping unauthorized access. After reading and discussing cases like Google Street View, Meta using public posts for AI training, and other data privacy issues, my view became deeper. I started to understand that privacy is not only about whether information is "public" or "private." It is also about context, consent, and how information is collected or reused. Something can be technically available online but still feel wrong if a company uses it in a way people did not reasonably expect. This matters in cybersecurity because professionals often have access to sensitive information, logs, devices, and user behavior. Just because I may have the technical ability to access data does not mean I should treat that access casually.

My future self should would take away that privacy is about respecting people, not just protecting data. In cybersecurity, I should always ask whether data use is necessary, fair, and clearly understood by the people affected.

A second topic that changed my thinking was corporate responsibility, especially through the Equifax breach case. At first, I saw data breaches mostly as failures of security controls or poor technical management. This class helped me see that breaches can also reflect ethical

failures in how companies prioritize profit, risk, and responsibility to the public. Equifax had access to extremely sensitive financial information, and many people did not choose to have their data stored there in the first place. That made the harm feel different from a normal customer relationship. Through the course material, including discussions connected to corporate social responsibility, I started to understand that companies have duties beyond simply making money or following the minimum legal requirements. When a company collects and profits from people's data, it also takes on a serious responsibility to protect that data.

This topic is very relevant to my career because cybersecurity professionals often work inside organizations that may be balancing security needs against cost, speed, or convenience. I may one day be in a position where I have to explain why a system needs patches, monitoring, better access control, or stronger protections. This course helped me realize that those recommendations are not just technical opinions. They are also ethical responsibilities.

My future self should would take away that weak security can become an ethical failure when people are harmed by risks that an organization could have reasonably reduced.

A third topic that stood out to me was Kantian ethics and treating people as ends, not just as means. This became especially important when thinking about cases involving data scraping, AI training, hiring, and automated decision-making. Before this course, I thought about technology mainly in terms of efficiency and results. If a system helped a company make decisions faster, I might have seen that as a positive thing. But using Kantian ethics helped me see that the process matters too. If people's data is used without meaningful consent, or if algorithms make decisions about people without transparency, then those people may be treated more like tools than human beings.

This changed how I think about cybersecurity and technology careers. In the future, I may work with systems that collect user activity, monitor threats, or analyze behavior. Those tools can be useful and necessary, but they can also become harmful if they ignore human dignity. Security should not become an excuse to over-monitor people or remove their ability to understand how their information is being used. Ethics adds a human layer to technical work.

My future self should would take away that people should never be treated as just data points, risks, users, or accounts. Every technical decision should still respect human dignity.

Overall, this course helped me connect ethics directly to cybersecurity. I learned that protecting systems is not enough if I am not also thinking about the people connected to those systems. Privacy, corporate responsibility, and human dignity are all issues I will carry into my future career. This course made me more aware that cybersecurity professionals are not only defenders of networks. They are also people trusted with protecting information, reducing harm, and making decisions that can affect others' lives.