In the world of cybersecurity, figuring out the difference between right and wrong is not always black and white. It is like navigating a maze of ethical and moral principles that constantly shape our decisions. Ethical principles, which are the rules society sets for us, and moral principles, which are the rules we set for ourselves, both play a big role. While in the cybersecurity world, constantly facing these situations, it is a necessity to balance these principles. For example, if there were a flaw in a popular software, following ethical guidelines, one might feel compelled to disclose it, even if it causes chaos. However, it may be required to access sensitive information to identify vulnerabilities, which may go against a person's morals which tell them to prioritize privacy. These decisions are not just about rules; they are influenced by who we are. Our backgrounds shape how we see the world, what we believe is right, and how we weigh ethical versus moral considerations. This is why courses like this one are important, because it gives everyone a baseline to think about before encountering any problems in the real world.

My upbringing was deeply rooted in the Catholic faith. My family attended mass and other church gatherings regularly, and I went to religious education once a week. These environments instilled in me a set of moral principles rooted in compassion, honesty, and integrity. However, when I was around 10 years old, my family stopped going to mass, and I stopped going to religious education. I was removed from the environment, but I was still rooted to the morals I had learned. Then, I went to a Catholic high school, and I was immersed in the community again. Now, I had both my personal morals, but also the ethics like a dress code surrounding school uniforms and haircuts. Today, I still do not go to mass and I m no longer at a Catholic school, but as I already mentioned, my morals have been instilled in me for as long as I can remember, and the ethics in the academic community mostly stayed the same, too.

Similar to the trolly problem that was discussed in class, which is a widely used moral/ethical dilemma because of how broad or specific it can be based on the application, other hypothetical situations can help us decide when to listen to ethics and when to listen to morals. For example, a situation that would be guided by ethics is a critical vulnerability in a widely used operating system. This vulnerability has the potential to allow malicious actors unrestricted access to sensitive user data and could be exploited for widespread cyberattacks. There are many ethical complexities of vulnerability disclosure, you face a dilemma: on one hand, there is a pressing need to alert users and software developers about the vulnerability so they can take immediate action to mitigate the risk. However, disclosing the details of the vulnerability publicly before a patch is available could also alert hackers to exploit the vulnerability, potentially causing significant harm to users. On the other hand, depending on the company and who cares in the company, the situation might not get fixed unless it is leaked to the public. Striking the right balance between transparency and responsible disclosure becomes a delicate task, as the urgency of fixing the vulnerability against the potential harm that premature disclosure could inflict on unsuspecting users is weighed. This situation should be solved ethically because while personal morals may align with the desire to protect individuals from harm, the ethical dilemma in this situation arises from external factors such as the potential consequences of disclosure on a broader scale.

A hypothetical situation that would be guided by morals is a cybersecurity consultant hired by a large corporation to assess the effectiveness of their security protocols. A part of the evaluation process is social engineering tactics to test the company's resilience against human manipulation. Making convincing phishing emails, making pretext phone calls posing as IT support, and even attempting to physically infiltrate secure areas by tailgating employees. However, one might question the ethical implications of their actions. While the goal is to

identify vulnerabilities and strengthen the company's defenses, the methods used involve manipulating individuals without their full awareness or consent. This raises concerns about the potential psychological harm inflicted on employees who may feel deceived or violated upon discovering the ruse. The delicate balance between conducting thorough security assessments and respecting the rights and well-being of those involved is very important. This is a moral issue because ethically this is a standard procedure for someone performing social engineering tests. However, the person internally questions whether their actions will end up with a net positive result. If the psychological harm brought to employees outweighs the knowledge gained about where the biggest vulnerabilities are, is it truly worth conducting the tests?

In conclusion, the world of cybersecurity presents a complex landscape where ethical and moral principles intersect, often guiding decision-making processes in intricate ways. While navigating the maze of principles, it becomes evident that the distinction between what is right and wrong is not always clear-cut but rather influenced by a large number of factors, including societal norms, personal beliefs, and professional obligations. The examples provided, such as the ethical dilemma of vulnerability disclosure and the moral implications of social engineering tactics, underscore the nuanced nature of ethical decision-making in cybersecurity. Furthermore, the interplay between individual backgrounds and upbringing adds another layer of complexity to these considerations, shaping perceptions of right and wrong and influencing how ethical versus moral considerations are weighed. Ultimately, courses like this one serve as invaluable resources, providing a baseline for ethical reasoning and critical thinking that can act as a guide through the myriad challenges in the real world. While continuing to grapple with these ethical complexities, it is essential to remain mindful of the broader implications of actions, ensuring that the well-being and security of individuals and communities in our pursuit of technological advancement is prioritized.