Raneem Alarian
August 5, 2025

Reflective Writing Assignment

Throughout this course, I've encountered a wide range of perspectives and concepts that have reshaped how I think about ethics, cybersecurity, and technology in general. There are three concepts in particular that have not only deepened my understanding, but will also continue to guide how I approach ethical decisions in my future career. These include professional ethics through the lens of the Ethics of Care, John Rawls' "veil of ignorance," and the framework of consequentialism. Each one offered new insights into what it means to act responsibly in a field where decisions can have wide-reaching consequences.

A lesson that stood out to me most in this course was gaining a deeper understanding of professional ethics, especially through the lens of the Ethics of Care. Prior to this course, I was under the impression that being an ethical professional is about following workplace rules and avoiding trouble. However, this class has helped me understand that professional ethics is about how my work as a professional impacts others, especially those who are vulnerable or trust us to do the right thing. Learning about Sourour's case reminded me how important it is not to lose sight of the human side of what you are doing at work. What also resonated with me is that ethics isn't just about following rules blindly just because you are told to do so by your company or boss. It is about recognizing and implementing the trust that people put in professionals such as cybersecurity experts. To be trustworthy in a field such as cybersecurity is to ask questions, speak up, or even pause to reflect on small acts that can make a big difference. What I hope to carry forward is the idea that being a responsible professional sometimes means doing more than just what's asked. It can mean challenging something that feels wrong, even if it's uncomfortable. To me, that's what real care and responsibility look like in a career.

Another idea that really challenged and expanded my thinking was John Rawls' "veil of ignorance." Before this course, I hadn't heard of it, and it seemed abstract at first. But the more I studied it, the more I saw how practical and powerful the idea really is. The concept asks you to design laws or systems as if you have no idea where you'll end up in society—rich or poor, powerful or powerless, tech-savvy or not. In a cybersecurity context, this means creating security policies and digital infrastructures without knowing if you'll be the one with admin rights or the one being tracked. It pushes you to think about fairness from a position of humility. For example, a fair digital system must protect privacy and provide access equally, not just to those who can afford it or understand it. What stood out most to me is how this principle forces designers and policymakers to center the needs of the most vulnerable, rather than assuming a "one size fits all" solution. A major takeaway from this perspective is that equitable digital protections are not a luxury, but a basic right. Going forward, I want to use this idea as a checkpoint: would I still think this policy is fair if I were the least advantaged user in the system? That question alone can help cut through bias, privilege, and convenience.

Raneem Alarian
August 5, 2025

Lastly, I've gained a better understanding of consequentialism and how it applies to cybersecurity. I had always heard the phrase “the ends justify the means,” but I didn’t really connect it to an ethical theory until now. I now understand that Consequentialism analyzes if an action is morally right or wrong based on the outcome of that action and not just what the rules say or what the person's intentions were. This theory applies to cybersecurity, as the field consists of constantly weighing out different options. As someone who anticipates working in cybersecurity, I might face a situation where I have to decide whether keeping systems running smoothly for users is worth the added risk of delaying a security update, for example. Although Consequentialism doesn't provide us with direct answers, it helps us think critically about the choices we make by evaluating their real-world effects. What I appreciate most about this ethical theory is how it demands accountability. In other words, one cannot hide behind their good intentions if the outcomes of their actions cause harm. This is a good reminder that thinking ethically should not stop at planning. My key takeaway from this is that in cybersecurity, making ethical decisions means paying close attention to what actually happens as a result of those decisions. Whether we’re creating software, enforcing policies, or responding to a breach, we need to constantly ask: who is affected, and how?

Overall, this class has provided not only a deeper grasp of cybersecurity ethics, but a deeper respect for the focus and responsibility that is present in this field. Ethics is not merely compliance, but relationships, justice, and consequence. I now have a better sense of how to think abstractly, ask appropriate questions, and understand that my decisions, although technical, have moral weight. I hope for my future self to recall on these lessons and use them sympathetically, justly, and with a clear-eyed view of outcomes.