There are a number of things I learned throughout my time in this class. One such thing would be product safety law and how it relates to a number of factors beyond what one may intuit on their own. Before this class, I wasn't familiar with the development of "strict liability" and the history of product safety law. While I am relatively familiar with certain parts of modern safety law and tort law, I have not really questioned much about them. I had not considered that there was a time when it was very different and standards and procedures were set up entirely differently. This may seem like a small and minor revelation, perhaps a fun fact to learn, but I believe it provides more insight than what may first come to mind. To me, learning more about the developments, the similarities to modern developments, and the ethical and legal reasons for such developments provides a wealth of insight that can be applied to all manner of situations. It helps me better understand the mistakes of the past and how we, as a society, seek to fix them in the present. It also helps me better understand how businesses operate today and how they apply business ethics and principles to actual operational procedures. Grimmelman used this previous development in product safety to detail current problems with consumer privacy in a cyber context. I feel as if his insights, in addition to the other insights within the chapter, could further my own understanding and hopefully allow me to make my own judgments about business and ethics in the future.

The fourth chapter, about professional ethics, also helped deepen my understanding of a number of issues relating to cybersecurity. One such insight, which I think was helpful, was the comparison and look into how both different institutions and professions address the same or similar concerns. The fact that relatively similar institutions could have massively different codes of ethics was one such insight. Also, important was the comparison across different fields as it relates to privacy and cybersecurity. I think one takeaway from the differences across fields is that cybersecurity, while it could be viewed as one topic, is not a unified, one-size-fits-all type of practice. The health field and the accounting field will both see their own specific intricacies and unique needs interact with cybersecurity and privacy concerns in their own unique ways. Expecting the exact same principles to be held up across the entire spectrum of professions is not only foolish, but may not necessarily be ideal either.

I also feel like chapters 6 and 7 provided a bounty of useful information that helped me understand a number of concepts far better. We often hear in the media about cyberwar, disinformation campaigns, and information warfare, but often, various terms like these are grouped together or confused. I believe both chapters helped me better understand what cyberwar and information warfare are, what they could entail, and how they have presented themselves in the recent past. This understanding could then likely help me better understand

how to approach future cyberconflicts and disinformation campaigns, see the signs, and identify them much more quickly. Overall, I greatly value these insights and others, as they have helped deepen my understanding of what the ethical questions are, how they are often approached in the real world, and other ways they could be approached in the future.