Old Dominion University

School of Cybersecurity

Jacen A Davis

PHIL 355E: Cybersecurity Ethics – Final Reflection

My overall experience with this course has led me to reflect on three critical topics related to professionalism and individual liberty: privacy, professional code of ethics, and whistleblowing. Privacy concerns individuals maintaining personal lives free from scrutiny and judgment from prying eyes within public, government, or business interests. Moreso, privacy, as I have learned, is self-constitutional or a complete whole itself, as it is privacy that creates privacy. Under a code of ethics, I can draw upon inspiration on how to be a successful IT and Cybersecurity professional and ensure my responsibilities to creating, maintaining, and operating a successful program that conforms to laws and regulations and ensures individual liberty and privacy rights are not infringed. Finally, I learned about whistleblowing as a tool and a fundamental concept of freedom to right wrongs and as a warning, when done from malice or poor judgment, which can create grave national security risks. Tying all topics together were the moral and ethical tools that help interpret moral dilemmas and prescribe general directions on handling them. Each ethical concept I learned came with pros and cons to their moral reasoning, which must be recognized and accounted for when utilizing them to make informed ethical decisions.

Privacy is a self-constituting system, as learned from Luciano Floridi and his work describing the constant informational friction of our modern ICT-driven society. Under Floridi, privacy is in continuous conflict between members of the informational sphere (Infosphere) known as Inforgs (informational organisms) and the informational entities that occupy, govern, and manage the flow of information (e.g., U.S. government, tech giants – Facebook, Google, Microsoft, Twitter, etc.). The availability of information versus the desire of entities and Inforgs to keep it confidential (private) is central to Floridi's arguments for the frictional nature of privacy. In my analysis of Google's Street View (1.4 Case Analysis on Privacy), I learned various viewpoints from Floridi and James Grimmelmann on traditional and novel solutions to privacy (Floridi – reductionists, ownership-based; Grimmelmann – privacy as product safety). Together, I understood that privacy, as a self-contained system, must drive the solution to the privacy debate. Because privacy balances with functionality and releasability of the necessary information to facilitate services, I understand that releasability and request for information must be consent-based and informative. If an organization I work for needs information from users, those said users need to be informed of their rights, responsibilities, and ability to consent or deny such requests.

To ensure that I, as a future IT/Cybersecurity professional, can preserve such rights to users as maintenance and guarantee of privacy, I must abide by a code of ethics. Regardless of if I serve as a member of a particular organization (IEEE, ACM, NSPE), working independently, as an employee, or as a public servant, I must abide by some form of professional code that is either compelled by an organization, employer, nation, or myself. I must protect the privacy and confidentiality of entitled parties according to established laws, regulations, and standards. As I have learned, professionals cannot operate entirely with the purpose of self-profiteering from their position or responsibilities. Depending on where one serves, such actions can have negative professional, legal, and national security connotations. In addition, professionals must be mindful of their actions and understand when their work will produce harm and stop their work from creating said harm either through adjustment of the product or revocation of services. One primary example where a code of ethics is required is conducting penetration testing. A professional hired to handle such a task requires the utmost discretion and strict adherence to procedures and policies. Suppose a professional "pen-tester" fails to adhere to standard-operating-procedures (SOPs), does not seek proper consent, exceeds the scope of the test, or does not undue any backdoors and exploits after the test. In that case, those are violations of ethics. Such a professional is expected to seek written and verbal consent from an authorized representative of the client, follow strict SOPs, conform to the scope of the assignment, and ultimately report findings and reverse any harm done to a client's IT infrastructure. As a cybersecurity professional, failure to do what is right and fair to clients and customers betrays their trust and a professional's upholding of the organization's cybersecurity mission.

Another topic along a similar vein to code of ethics is whistleblowing. As I have learned, whistleblowing is a tightrope balanced carefully as an IT/Cybersecurity professional. The line between identifying a clear wrong that harms others and harms the mission and standing of an organization and indiscretion and negligence on the part of the whistleblower is razor thin. Examples of those who have engaged in whistleblowing serve as prime subjects for whistleblowers ending up on the wrong side of their actions. Edward Snowden identified a failure of the National Security Agency to restrain the collection of millions of American call data logs, which the secretive FISA courts ruled illegal and potentially unconstitutional. However, he leaked swaths of other classified information and then fled the country to eventually reside with the U.S.'s chief European adversary, the Russian Federation (Russia). Chelsea Manning, who helped leak video of U.S. Apache crews killing innocent civilians and two Reuters journalists in a case of accidental civilian fire, also leaked other classified documents along with the video to WikiLeaks. WikiLeaks had dual motives for working with Chelsea Manning, seeking both the video and additional classified information, using her to get more

classified docs to leak. In both cases, they failed to execute proper judgment, as I had found (regardless of others' failings) in my Case Study and Case Analysis.

One theme tying all three topics (privacy, code of ethics, and whistleblowing) together is the importance of professional conduct and professionalism. As a future and burgeoning IT/Cybersecurity professional, how I act and believe when I act is critical. Unprofessionalism and poor conduct could compromise one's judgment and decision-making process. That could cost a company profits and satisfied customers in the civilian corporate world. In the world of national security and public service at the Federal, State, Tribal, and Local levels, it could easily cost people's lives. Based on this theme, one ethical viewpoint comes to mind: consequentialism. Consequentialism is all about the consequences of one's actions and making the best-informed decision from knowing the consequences of your choices. A vein of this moral theory I learned from this course was Utilitarianism, which focused on making choices that brought the greatest happiness (common good) to the greatest extent possible, be with people or with those that are not (animals, plants, ecosystems, etc.). I must understand the consequences of my decisions concerning the state of an organization's IT and cybersecurity program as the safety of personal data (PII/PHI), intellectual property, or national security information (classified information, intelligence, tradecraft) is at stake. Making an ill-informed choice, even at the smallest level, could have repercussions leading to compromise to the greatest extent. As a rising professional, there will also come a time when I will be given responsibilities over a program, project, or people, and it will be my responsibility to ensure the greatest extent of coworkers, customers, and stakeholders are satisfied while providing code of ethics are not breached, and my professional conduct is not compromised.