Zach Weaver
CSCI 325
Ethics Paper
11/5/22

Handling Ethical Issues from a Biblical Perspective

Have you ever been faced with a decision that could affect the well-being of yourself and others? A decision that, if executed poorly, could lead to severe repercussions that violate your moral and ethical beliefs? Unfortunately, these types of decisions are made daily by many computing professionals around the world. In the ever-changing fields of computer science and cybersecurity, the subject of ethics and how to handle ethical issues must be understood to prevent severe or immoral consequences. Some of the most prominent ethical challenges that I might face in my career include handling important personal data safely and rationally or working with unrestricted administrative access to a company-wide system. It is essential to understand how to prepare for situations like these so that, when they do arise, I am equipped to make ethically sound decisions that align with ethical codes and my own moral and biblical beliefs.

One of the most prominent issues I believe I will face in the industry will involve handling important company data for a large organization like a hospital system. The healthcare industry is known to be a huge target for cyber attackers looking to steal or use personal medical data, which means handling that data needs to be done safely to ensure it doesn't fall into the wrong hands. An article written by Maryville University on the subject of cyber ethics explains how "According to the U.S National Library of Medicine, computers have played a role in the healthcare industry since the 1960s" (Ethical Issues behind Cybersecurity). Let's suppose, for example, that I am employed by a healthcare system and tasked with working with private patient information. Handling this type of sensitive information would give me a choice to use the data for my agenda or to continue operating according to the organization I am working for. I must handle the data entrusted to me safely and honestly to ensure it doesn't get into the wrong hands. Especially in the healthcare industry, fraudulent attackers often try to use this type of patient data to forge IDs to do things like buying and reselling drugs (Humer, Caroline, and Jim Finkle). This could be a serious refraction that could easily be avoided by operating ethically and not maliciously manipulating any data. Section 1.6 of the ACM Code of Ethics states, "Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups" (ACM Code of Ethics and Professional Conduct). Using patient information for my own means would be a direct violation of this code of ethics and result in serious moral and legal consequences.

The question then arises, how should one prepare for situations like these, and what actions should be taken so one may be equipped to make sound-minded decisions? One of the best ways to prepare for unforeseen cybersecurity situations is to ensure all those involved are well informed of the procedures being done and perform those procedures in a selfless manner that promotes honesty. This could be anything from informing a manager of any system vulnerabilities to letting customers or patients know that their information may have been stolen in a data breach (Ethical Issues behind Cybersecurity). According to section 1.3 of the ACM Code of Ethics, "A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties (ACM Code of Ethics and Professional Conduct). Although it is important to maintain a level of transparency with those involved, it is equally important to maintain a strict amount of confidentiality in order to prevent any sort of data or security breach (Ethical Issues behind Cybersecurity).

In addition to making sure those involved are aware of what I, as a computer professional, am doing to aid their system, I must also be prepared to handle situations honestly, not giving private information the benefit of the doubt. In his article titled "Ethical Problems in Computing," Lou Berzai explains how computer professionals can act one of two ways when faced with an ethical decision. They can either assume information is in the public realm until there is some evidence that it is not or assume that information is private unless or until there is evidence it is not. Out of these two, the appropriate course of action would be to assume that the data being handled is private, preventing any leak or mishap in the future. One of the most considerable challenges surrounding the field of cybersecurity is realizing that there truly is no fundamental mechanism for enforcement regarding what is and is not allowed. Living during a time when open-source code is readily available to anyone on the internet means that computing professionals need to take great caution in what actions they perform. Taking the proper precautions and preparing for ethical challenges is a great way to help prevent any possible malicious consequences.

I believe that having a biblical worldview is foundational to having sound ethical principles, especially in the world of cybersecurity. This can be seen prominently within specific ethical codes such as the ACM Code of Ethics and Professional Conduct or the IEEE Code of Ethics. Section 1.7 of the ACM Code of Ethics emphasizes the importance of confidentiality. Working as a computing professional means there will be opportunities to use data or other types of information for something different than what was initially intended. Section 1.7 states that "Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, or organizational regulations, or of the code" (ACM Code of Ethics and Professional Conduct). Section 1.7 lines up with the fundamental premise that computer professionals should handle any data they are working with the same way they would want their own data dealt with. Luke 6:3 says, "Do unto others as you would have them do unto you"

(NIV). When faced with an ethical decision, one should always consider the rationale behind each possible outcome. In his article, Berazi goes on to write, “Computer professionals should have an obligation to use the information they have access to in a proper manner, but some choose to use this information immorally to the detriment of others” (Berzai).

Similarly, it is critical that those working in the field of cybersecurity act out of integrity and honesty. In some situations, this can be hard to do because often, our natural human inclination is not to consider the best interest of others. As a Christian, however, it can be comforting to remember that we are not alone in fighting temptation and making tough ethical decisions. In the bible, Paul exclaims, “I can do all this through him who gives me strength” (Philippians 4:13 NIV). Additionally, section I of the IEEE Code of Ethics describes the importance of upholding the “highest standards of integrity, responsible behavior, and ethical conduct in professional activities” (IEEE Code of Ethics). Operating with a high level of integrity coincides with part of chapter two in the Book of Titus, which explains that, in everything you do, it is vital to set an excellent example through integrity and honesty so that no one can say anything wrong about you or those involved (Titus 2:7-8 NIV). Understanding how closely related ethical principles are to scriptural morals is important because it allows one to keep a biblical worldview when faced with questionable workplace situations.

Pursuing a career as a cybersecurity professional will undoubtedly involve ethical dilemmas. Knowing how to prepare for and react to these situations will allow me to ultimately make decisions that not only align with ethical codes but my personal spiritual convictions as well.

Works Cited

"Access Your Bible from Anywhere." *BibleGateway.com: A Searchable Online Bible in over 150 Versions and 50 Languages.*, https://www.biblegateway.com/.

"ACM Code of Ethics and Professional Conduct." *ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics*, https://ethics.acm.org/.

Berzai, Lou. "Ethical Problems in Computing." *Default*, 5 Oct. 2022, https://www.comptia.org/blog/ethical-problems-in-computing.

"Ethical Issues behind Cybersecurity." *Maryville Online*, 5 Jan. 2021, https://online.maryville.edu/blog/cyber-security-ethics/.

Humer, Caroline, and Jim Finkle. "Your Medical Record Is Worth More to Hackers than Your Credit Card." *Reuters*, Thomson Reuters, 24 Sept. 2014, https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

"IEEE Code of Ethics." *IEEE*, https://www.ieee.org/about/corporate/governance/p7-8.html.