Charlotte Strobl

Professor Henderson

CSCI 325 – Object Oriented Programming

2 December 2023

Ethical Dilemmas in Cybersecurity

When it comes to cybersecurity, one may encounter various ethical dilemmas on the job. These issues include but are not limited to confidentiality, security, and privacy. One in the field may find the temptation to reveal whatever information they stumbled upon while securing someone's data. When in the role of securing someone's data, a great responsibility and burden is placed upon that person. This field involves deterring hackers and viruses, which, if failed to prevent, would be detrimental to the client. Luckily, the ACM and IEEE codes of ethics provide professionals with a foundation for ethical decision-making regarding these issues. When faced with finding a balance between security and human rights, I can refer to biblical principles, case studies, and codes of ethics to guide my actions.

In cybersecurity, there is often a trade-off between security and human rights. An example of this is online activity monitoring. If the government tracks the internet activity of citizens, they could use the information collected to locate terrorist threats much more effectively, but this hinders civilians' right to privacy. According to Taddeo, "The need to strike a balance that would allow for reaching an ethical equilibrium between cyber security measures and individual rights is then compelling and is a concern that crosses the boundaries of academia" (354). If the government tracks internet activity to the extreme, it fails to balance the security measures with individual rights by trading one for the other. Users put tremendous trust

in a system to keep their data private, but security breaches hinder that trust. Because of that, there must be an ongoing dialogue that considers preserving individual rights while additionally providing sufficient security. However, there is no one simple fix to this due to technology's rapid changes. According to Pawlicka et al., "The discussion on the ethical dilemmas of cybersecurity must continue, and the list has to be updated, preferably in the form of an inter- and multidisciplinary dialogue. Then, the outcomes of the discussions have to be transformed into meaningful actions" (5). This suggests that cybersecurity ethics must constantly be revised to keep up with technological advances. Amidst these changes, there needs to be a balance between security measures and respecting human rights.

When taking a hard look at myself, I realize I am not prepared to take on these challenges. I feel as though I would not even know where to begin when addressing a detrimental situation regarding implementing good security while considering human rights. However, I would approach this by researching. Bustard suggests examples of real-world cybersecurity scandals help to explain the impact of misuse on an organization (694). I would make the effort to look into real-world cases and find what works versus what does not. In addition, I will align my decision-making to principles from ACM, IEEE Codes of Ethics, and biblical principles.

The ACM and IEEE codes of ethics share striking similarities to biblical principles. Both codes of ethics mention avoiding harm, acting justly, and being honest. These line up with scripture because the Bible tells Christians to "love your neighbor as yourself" (Matt. 22.39) and to "walk with integrity" (Prov. 10.9). When someone actively loves their neighbor, that person will protect their privacy rather than invade it, act justly instead of unjustly, and look to protect them from harm. Likewise, when someone walks with integrity, that person will be fair,

trustworthy, honorable, and not deceitful. In other words, one who earnestly obeys the teachings of the Bible will consequently adhere to the ACM and IEEE codes of Ethics due to their overlapping concepts.

In short, finding the balance between security and human rights is challenging, but one can use biblical principles, case studies, and codes of ethics to overcome this issue. Unfortunately, security solutions are not a one-time thing and require frequent revisiting as technology continues to advance day after day. Discussions revolving around these issues should be ongoing and continuous. Although I am currently new to this issue, I can utilize biblical principles and codes of ethics to verify my decision-making and look to previous cases to measure the success of a specific implementation. Accessing these resources will ensure that I promote effective security measures that protect people while also respecting their rights.

Works Cited

Taddeo, Mariarosaria. “Cyber security and individual rights, striking the right balance.” Philosophy &; Technology, vol. 26, no. 4, 2013, pp. 353–356, https://doi.org/10.1007/s13347-013-0140-9.

Pawlicka, Aleksandra, et al. “What will the future of cybersecurity bring us, and will it be ethical? the hunt for the black swans of cybersecurity ethics.” IEEE Access, vol. 11, 2023, pp. 58796–58807, https://doi.org/10.1109/access.2023.3283791.

Bustard, John D. “Improving student engagement in the study of Professional Ethics: Concepts and an example in cyber security.” Science and Engineering Ethics, 2017, https://doi.org/10.1007/s11948-017-9904-4.