Riley Osborne

CSCI 325

Prof. Julie Henderson

November 5, 2022

Object Oriented Programming Ethics Paper: Data Breaches

You work as a data scientist. Your job is to maintain all aspects of your data, with honesty, discretion, and diligence being key values to implement. Honesty is for openly sharing with users how their data is being used and stored. Discretion is for making quality decisions on how to deal with data security and storage. Lastly, diligence is for maintaining the level of maintenance required to constantly update your usage of data, security of data, and quality of data. The issue at hand in this essay is centered around privacy protection. What are the worldly and Christian sets of ethics dealing with users’ data protection?

The burden of a data scientist is hefty, and I predict my biggest obstacle to overcome will be carrying the burden and consequences from a data breach. In my scenario as data owner, I would most likely be held responsible for any cloud security data breaches (Nolan Whitehurst). This means that I must maintain premium security measures to my utmost ability, so my users’ data is not unexpectedly released or snatched by malicious hackers. The ACM code of ethics agrees, stating in section 1.6 that a computing professional’s duty includes not only proper collecting and storing of data, but also “protecting it from unauthorized access and accidental disclosure” (ACM). The IEEE code of ethics supports responsibility with privacy as well, prioritizing privacy so much that it gets mentioned within the very first principle listed under section one (IEEE). To visualize the gravity of data protection, picture this: your best friend gives you her phone PIN, which is private information to not be shared with anybody. Your ethical job regarding the PIN’s security is to keep it private by not telling anyone her PIN, not writing it down somewhere so that someone can steal it, and not using the PIN in any situation that would offer an onlooker the opportunity to shoulder surf and steal her PIN. This is a miniature thought process required to comply with the ethical standards of data security. In a professional setting, the burden multiplies unimaginably, because today’s technology allows data owners to hold private information for not just one best friend, but hundreds, thousands, or even millions of people simultaneously.

To overcome data breaches, a clear mindset and professional practices are necessary. ACM advises the integration of “mitigation techniques and policies, such as monitoring, patching, and vulnerability reporting” (ACM). In the case that your data protection scheme fails, both code of ethics unanimously advocate admission of fault and transparency. The IEEE agrees it is important to “disclose promptly factors that might endanger the public or the environment” (IEEE). Even though the IEEE is not specifically addressing the individual here, they are not implying the unimportance of the individual. They just wanted to write their principles very generically and inclusively. The ACM code of ethics is more helpful, clarifying that in addition to setting up security measures, “Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner, providing appropriate guidance and remediation” (ACM). As a perfectionist, I will never feel adequately prepared to defend whatever data I am responsible for, but I do have some guidance. “For the eyes of the Lord are on the righteous, and his ears are open to their prayer. But the face of the Lord is against those who do evil” (*English Standard Version,* 1 Pet. 3.12). God supports those with a sincere, righteous heart, and knowing that I do not have to fear. If I handle all data responsibly, with integrity, and give my best in doing so, I know that the Lord will approve of my endeavors.

With knowledge comes great responsibility, and knowing data needs to be handled and treated a certain way does not mean you know how to practically. A practical mindset for any implementation of cybersecurity is grounded in your perception of the enemy. 1 Peter 5:8 says, “Be sober-minded; be watchful. Your adversary the devil prowls around like a roaring lion, seeking someone to devour” (1 Pet. 5.8). I understand this verse is referencing our spiritual battle against satan, but this mind set works in cybersecurity as well. The “bad guys” have an advantage in technology. It is common knowledge that tearing down is easier than building up, and hackers are always getting smarter and more creative to work around the defensive barriers that are put up. They only need to find one crease to gain access. Therefore, it is beneficial to view hackers in the same way that satan is portrayed in this verse. The hackers are constantly prowling about, seeking to break into and steal data for their own personal gain, and it is necessary to be sober-minded and watchful concerning data security as well. With this thought process and the aforementioned principles, I would personally seek counsel and hire expert help that I can trust for my system’s data security. With experience and seasoned guidance, I would be able learn how to properly exercise data security myself. This would afford me the opportunity to either be directly responsibly by handling data security myself or implement a more efficient system where I can hire a cybersecurity team that I can hold responsible for data/system security.

It is important to point out that as helpful as the ACM and IEEE codes of ethics have been so far, they are fallible. The bible is the ultimate standard. For example, IEEE principle seven rightly instantiates fairness or lacking partiality as an ethical issue to uphold but is corrupted into including the worldly view of “sexual orientation, gender identity, or gender expression” into it. God is clear in the bible as having made only two genders: “When God created man, he made him in the likeness of God, Male and female he created them” (Gen. 5.1-2). I am in no way advocating to treat them disrespectfully or not as one made in God’s image, but if the idea of respect in the IEEE code of ethics consists of referring to an individual contrary to the way God created them, I can not comply. I can not disrespect God’s perfect design, being His very own image, by intentionally addressing a male as a she, a woman as a he, or address a person with pronouns such as “they/them”, “it”, “you all/we”, or whatever else.

The ACM code is not perfect either. For example, the ACM code of ethics has a slightly twisted perception concerning developer’s creative work (ACM). “Developing new ideas, inventions, creative works, and computing artifacts creates value for society, and those who expend this effort should expect to gain value from their work” (ACM). The bible teaches us that this is not the only way to view the world. “Do nothing from selfish ambition or conceit, but in humility count others more significant than yourselves. Let each of you look not only to his own interests, but also to the interests of others” (Phil. 2.3-4). Using this verse, we are not required to gain value from all our work. Sometimes the bible teaches us that our value is in serving Him by sacrificing our rights of ownership to serve others and engage with their interests. So if you want to create a program for someone anonymously or with no credit besides your name as author, that is a commendable way to serve others without expecting to “gain value” as a creator from it.

Works Cited

ACM Code 2018 Task Force. “The Code Affirms an Obligation of Computing Professionals to Use Their Skills for the Benefit of Society.” *Code of Ethics*, 2018, https://www.acm.org/code-of-ethics.

IEEE Board of Directors. “IEEE Code of Ethics.” *IEEE*, 2020, https://www.ieee.org/about/corporate/governance/p7-8.html.

*The Bible.* English Standard Version, Crossway, 2001.

“Who Is Responsible for a Cloud Security Data Breach?: DPP.” *Nolan Whitehurst*, 6 Apr. 2020, https://www.dpp-gdpr.com/news/cloud-security-data-breach/.