Draft

Scenario #5: To Test or Not to Test

In Scenario 5, a team of developers is tasked with developing a communications system in disaster zones for first responders. After going through the tragic events of 9/11, my fellow developers and I are passionate about this project with the hopes that it can truly help improve the efficiency and effectiveness of first responders in a disaster zone. The system will allow users to communicate with each other, supervisers near the scene, and with other emergency personnel. Being a mission-critical tool intended to be used by first responders in a disaster zone, our team realizes the importance of reliability. However, our boss, the project manager, has put us in a tough situation. The project timeline they have put together only describes a single testing phase to take place in a field near the company office. The field being used is just a spacious land of grass and a few trees. Additionally, to save time and money the software team will be playing the role of first responders. Our project manager firmly believes that this is the best course of action to meet the expected projected deadline. For the purposes of this paper, I will be assuming the role of a developer on the software team responsible for the communications system. My co-workers and I are deciding on to what extent are we sticking to the proposed testing plan.

There are a few entities involved and/or impacted by the development of the communications system. A vital party to consider being the end users, first responders. They are going to be heavily dependent on the system; therefore, they would be affected by any inadequacies evident in the final product. Considering privacy for a moment, the **Electronic Communications Privacy Act, ECPA,** protects all electronic communications of the system (Potasznik, Day 5). Since the first responders will be the majority of electronic communications data, they are the party most susceptable to privacy violations. Although this is an important aspect to keep in mind, I plan to keep the contents of this papers focused on the technical reliability of this system and decisions revolving the project's testing plan.

While the end users of this project is the first responders, the focus of the first responders will be the victims in the disaster zone. Therefore, somewhat indirectly, victims are also stakeholders. The victims will be at the mercy of code of ethics that would be applied by first responders that the time of a disaster. The reliability of the communications system is going to resonate through the first responders as their efficiency and effectiveness will determine the amount of people that would be helped in a disaster situation. A failure to ensure the reliability of the system is going to result in a lack of needed assistance. Additionally, since the victims are not part of the communications system channels, they will not need the ECPA protections that we would see at the first responder level. An exception to this is the scenario where first responders are discussing the situation of a particular victim, so the protections still apply in some form.

Being responsible for the development of this system, makes the company I work for a significant entity in this scenario. Specifically, the developers, including myself, and the project manager are the most involved when it comes to deciding and executing the testing plan on this particular project. For the purpose of this paper, the developers are associatied with **ACM** and **IEEE**, organization that have both adopted the Software Engineering Code of Ethics and Professional Practice (Potasznik, Day 22). Later in the paper, during the discussion of options, this particular code of ethics with be a reason to pursue an alternate testing plan in order to improve the overall reliability of the project.

The ethical issue being presented with the proposed testing plan can result in serious consequences for multiple stakeholders. A lackluster testing plan increases the probability for bugs in the codebase and bugs will result in errors during real use of the system. These errors occuring in a disaster situation could be detrimental to the effectiveness of the first responders and the safety of disaster victims.

The location of the system's testing is another issue with the plan. A disaster can happen anywhere, so it's important that the system is tested in many different environments. The robustness of a system is not going verified by testing it in a single field by the office. It is important to ensure that the system is going to operate properly in both urban and rural environments with plenty of open air space and almost none. To address this issue the best option will account for these discreptencies and improve the reliability of the sytem.

Lastly, when it comes to the company the team competency is dependent on the decisions being made around testing. Deciding to test in any particular way will shed like on the quality of work being put out by the developers and decision-making ability of the project manager. If we look at the initial plan with a single testing session happening in a field next to the office, we see a plan that does not put an ephasis on the testing aspect of the development process. This unfortunately foreshadows the quality of work of future projects developed by this team. If there is a lack of testing in one project, there will likely be a lack of testing in the next.

My fellow developers and I are scheduled to start the project soon and we must decide what is going to be our course of action. One option is to not change anything and stick with the current testing plan. On the other hand, we could go in the opposite direction and propose and execute an entire different testing plan. And as a final option, we could refuse to work on the project with it's current execution plan and leaking the state of the system if the company decides to move forward. I will take a look at each of the options an decide which would be best.

Looking at the first option, sticking with the current testing plan. This seems like the option of least resistance since there is a minimally valid plan ready to go. However, this option would most likely result in the issues and their ramifications discussed early in the project. Since the initial method of testing does not ensure the highest possible reliability and essentially guarentees an eventual failure in the system when applied to the right disaster, I would categorize this option as ethically prohibited.

The second option is to propose and execute a different testing plan. This plan of action starts with reminding your team of their membership to the professional organizations, ACM and IEEE, therefore informing them about there ethical obligation to apply the Software Engineering Code of Ethics and Professional Practice. With this code of ethics in mind there are two obvious aspects of the intial testing plan that would need to be changed. The first would be the inclusion of end users, real first responders, in the improved testing plan. Pretending to be first responders would not accurately capture the edge cases that are going to come with using this system. Secondly, the improved testing must be significantly more extensive. This is where the idea of unit testing needs to be introduced to ensure that every line of code is tested, resonating reliability throughout the codebase. Simultaneously, security vulnerabilitie must be a high priority focus point for the team. This would require extra effort being put in by developers, like assuming the role of a **white-hat hacker**, attempting to hack into their own project to ensure that any vulnerbilities are protected against in the final product (Potasznik, Day 12). Only when all of these steps are taken will there be mission-critical reliability of the entire communications system; therefore, I would label this option as ethically obligated.

The final and third opition, would be refusing to work on the project. This would allow for the possibility of the project continuing without me. In this case I must consider the **3 things to consider before leaking any information: the type of material, the value to society, and the risks to society and involved in individuals** (Potasznik, Day 7). The material is regarding a system that would be used in disaster zones and the value that it could have would save lives. If a non-reliable system is used in a real situations the risks could be extremely grave. In the worse disasters, like 9/11, there would be loss of life. Leaking the state a a system like this could potentially stop it from being used in a real situation. Since keeping the system from being used is a possibility in this option, I would categorize it as ethically acceptable.

After considering considering three different options, I would have to say that there second option is the best. Executing a different testing plan was categorized as ethically obligated for the benefits that come with more robust testing methods. It is understandable that there is a significant amount of additional work required to complete this option successfully. The types of work hours required by this option would not be easy or possible by everyone on the team. However, if we were to assume that the team and I were to subscribe to **utilitarian reasoning**, the pain and suffering that would come with the additional work would be outweighed by the communications system's reliability in a real disaster situation (Potasznik, Day 2).