Project P:

Evaluation and Redesign

of RFID Access Control

Michael Tong
mtong31@gatech.edu

Abstract. The RFID badge system is evaluated in accordance with HCI principals and a redesign is proposed to improve its shortcomings. Redesigning the interface to incorporate a facial recognition system is discussed and justified as an alternative interface to address those flaws.

Introduction

Prevention of unauthorized access to restricted areas if often accomplished by physical keys, and more recently, radio frequency identification (RFID) badges. While these badges may appear to work like magic, sending information across the air to unlock a door, they are relatively old technology developed nearly half a century ago in 1970 by Mario W. Cardullo and William L. Parks III (Cardullo 1973). They may be more advanced and provides a quick and somewhat simple alternative to the primitive key (Potts 1990), they still suffer from inefficiencies and irritations for users. This report analyzes a potential alternative to supplement the RFID badge for physical area entry.

Heuristic Evaluation

RFID badges provide a solid alternative to traditional keys which both share the goal of providing a specific person access to a restricted area. In comparison with the traditional key, RFID badges bridge the gulf of execution quicker by decreasing the number of actions required as well as easing the precision of execution. This often makes badges more comfortable to use since it increases the invisibility of the interface, reducing fatigue. Lastly, badges are more tolerant than keys, where if a badge is lost, the system can simply be reprogrammed to prevent access from that specific badge, whereas with keys, the lock has to be replaced. In comparison with the traditional key, the badge interface works better by utilizing the flexibility and operational efficacy of electronics.

When analyzing the gulf of execution for a RFID badge, nearly every stage of the process is reduced. The identified intentions are similar however in that the user still probably understands that they need to unlock a door or gate to achieve their goal. Identification of actions needed to be taken does differ though. With the traditional key, the user identifies that they need to find the correct key, put the key inside the lock, turn the key to unlock the door, turn the key back, remove the key, then place the key back to where it was taken. In comparison with these actions, use of a badge requires the user to find their badge, place it on the badge reader, and return the badge to the original location. The sequence of actions required is less for the badge, and also requires less precision, which leads to the last stage in the gulf, execution. Users do not need to precisely place their badge on the reader while keys often only have one correct orientation to be used. Reduction in the gulf of execution for the badge over the key often makes it a good interface for access entry.

Primarily resulting from the gulf of execution being reduced, user ease is increased with the lowering cognitive strain and fatigue. As mentioned, keys require more precision to be used, and due to their physical mechanisms, may deteriorate over time, reducing performance, and increasing mental fatigue. Many people may be able to

relate to having instances when a key did not fit well, didn't turn correctly, and/or required a lot of slamming and reattempts before it would function properly; situations often stressful and irritating. Use of a badge alleviates these issues by using electronics which do not deteriorate as quickly due to the non-physical interaction of the mechanisms, ultimately reducing the user's cognitive fatigue.

The tolerance of RFID badges is also larger than the traditional key. Since these items typically exist as relatively small objects, the opportunity to lose them is fairly high. With badges however, their primary mechanism is a low-cost electronic sensor that can be reprogrammed very easily and cheaply. This allows companies to produce generic badges in bulk and program them as needed. When replacing keys however, there does not exist a simple method to "reprogram" a generic key into a replacement, often a specialist is required to craft a replacement. Additionally, when a key is lost, it poses a security risk since unauthorized users now have access to restricted areas. With a badge, most systems can remove the specific badge's access when issuing a replacement. Keys do not have that simple luxury and require the lock(s) to be replaced. While badges do have the advantage over keys in terms of tolerance, when these items are lost, regardless as a key or badge, there becomes the inconvenience of the user not being to achieve their goal without either going out of their way to replace them or having an escort; they still exist as objects that can be lost.

RFID badges overall are an improvement to traditional keys, but they still suffer from fallacies. Badges and keys are designed to provide a specific user access to an area, so why is there a need for anything more than the user's presence? The need for a separate object decreases the invisibility and simplicity of the interface; users have to be cognizant of remembering their badge or key. Achieving the goal of providing a user access to a particular area should be reduced to only needing the person there and present, not an object to represent a person as being qualified. This restriction imposes unnecessary constraints on the user and also reduces the simplicity of the system, which can be improved.

As a result, badges pose a lot of unnecessary constraints. In order to be used, the user must remember to carry it with them. They can be simpler and more invisible. The purpose of a badge is to prove that a user is someone who is supposed to have access to a location, and generally speaking, no two people are the same, which makes the individual unique like a key. These constraints exists because of the supplemental need for an additional object in addition to the user as verifying proof of credentials.

In addition to the constraint of needing to carry a badge, they are often not flexible across different systems. To gain access to different areas, different badges are sometimes needed, similar to how different keys are needed for different locks. In these situations, the inconvenience of a badge is escalated to the user needing to remember which badge belongs to which specific system in addition to the physical capacity of having to keep track of more than one key, all which have the similar goal of proving the user's identity. These issues are often the result of incompatible badge reading systems.

While the badge system significantly improves the traditional key and lock system by reducing the gulf of execution, increasing ease, and increasing the tolerance of the system, there still exists room for improvement. With the advent of modern computation and a greater understanding of human computer interaction principals, the badge system can be improved to alleviate the issues surrounding simplicity, unnecessary constraints, and flexibility, while maintaining the benefits over the traditional key system.

Interface Redesign

To address the fallacies in the RFID badge system while attempting to preserve the benefits of it over the traditional key, this analysis proposes the use of a facial recognition system with modern computational techniques. This redesign does not completely replace the RFID system but will supplement it by integrating a high-

resolution camera to allow users the option of using either system. This addition allows for users to maintain their current mental model of the system with the redesigned system there to be discovered. In addition to the camera, it will also contain storage for maintaining the computational algorithms and facial data of authorized users. Figure 1 below displays a traditional RFID badge system alongside the considered redesign. Form factor increases are kept minimal as to maximize compatibility and comfort, and the camera could potentially be integrated into the badge reader's frame.

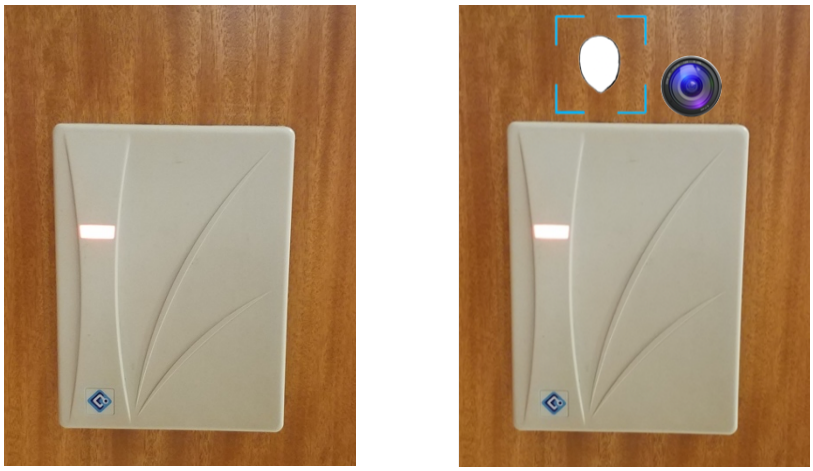

Figure 1: Left: Original Interface. Right: Redesigned Interface (actual camera and icon size may vary)

The camera is placed above the RFID detector since the detectors are often at waist level and placement of the camera higher up will allow it to better capture the faces of people. Alternatively, the camera can be placed on the sides of the detector if physically required for implementation. Placement of the camera below the detector would be suboptimal for facial detection, due to the angle of image capture possibly not being able to assess the user's entire face.

To use the system, users will simply have to look at the camera, which will utilize computational algorithms to determine if the facial feature dimensions matches one in the storage system of authorized users. The machine will then promptly provide access if there is a high confidence in the match and continue scanning if there is not

a match. Metadata containing logging information will also be stored and utilized for anomaly detection as a means to increase security.

Since the system is a hybrid, providing users access to either system, and that modern camera lenses are relatively small, signifiers will be implemented to improve discoverability in the event that they are not comfortable or familiar enough with the system. A simple symbol such as the one shown in Figure 2 below will be placed next to the camera as a signifier to encourage the discovery and use of the camera implementation. The color of the signifier should be adjusted to allow for clear visibility.

Figure 2: Camera icon signifier (color may vary to increase contrast)

In addition to the signifier, feedback to the user that they have gained entry is also necessary for a proper design. With most badge readers, there is an audible click or a light switches colors once the badge is read. Access with facial recognition can be performed in a similar fashion where a light indicator flashes green upon granting entry and is red or yellow otherwise. This light indication should also be connected to the existing system if it exists as to not confuse the user with multiple sources of feedback. Implementation of this design provides minimal but effective feedback as to not overload the user, quickly bridging the gulf of evaluation to the user. A prototype example of this implementation is demonstrated in Figure 3 below.

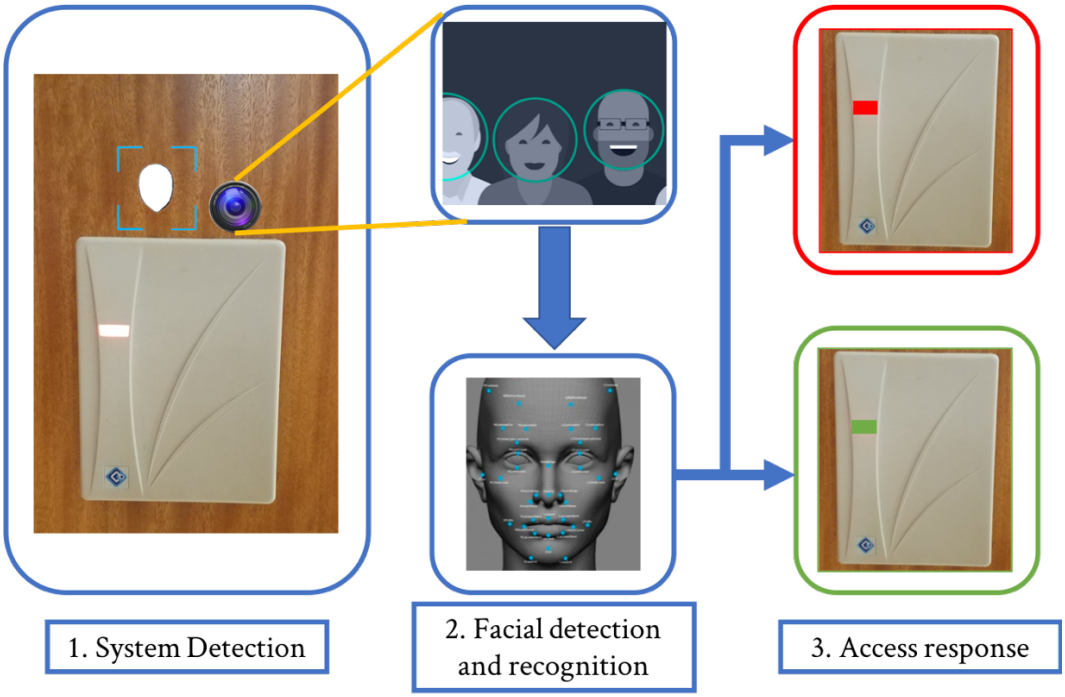

Figure 3: System light indicator (Cole, 2015; Keval 2017)

The badge reader will still allow users to use a card if they have a preference for it, given the assumption that some users may not want their facial data kept in the security system. This badge reader however will interact exactly the same as before, requiring the user to maintain a badge, but will share its light indicator with the camera if it has one.

Interface Justification

The primary justification for implementation of the redesigned badge system is to address the statement in the evaluation of how the goal is to provide an authorized user access to an area, and the addition of another object to supplement the user to perform that task is theoretically unnecessary. Additionally, badges inherently constrain users to remember carrying them when attempting to enter the secure location, which often cause frustration when forgotten or misplaced. From the

predictor point view of the user, these fallacies can be improved with the facial recognition system for entry by creating a more invisible interface.

Before this analysis continues to justify the redesign, needfinding is performed to reduce biases, mainly confirmation bias, and to better understand the user. A survey had been released to the public through http://peersurvey.cc.gatech.edu/, where 31 responses have been captured. The survey questions are high level and general to gain an understanding of both the usage of badges and respondent's superficial comfort with the proposed system. Survey questions and results can be found in Table 1 of the appendices. Respondent's personal information were not recorded, and it had been released to both the Georgia Tech community as well as the author's social media outlets.

The results were nothing short of astonishing. While 31 responses is certainly not a large sample size, every respondent stated that they use some sort of badge or access card, with 71% (22) stating that they use more than one badge. 77% (24) stated that they use their badge on a daily basis, 81% (25) have lost or forgotten their badge before, and 71% (22) find them inconvenient. From the free response (Question 4, *What do you dislike most about using an access card?),* the common response was the inconvenience of having to carry it and taking it out to use. One response in particular resonated well with the study, and was humorous, heartbreaking, and informative:

> "As a woman, I don't also wear pants. When I'm wearing a dress, my only options are to wear it around my neck or click to my neckline. The neckline approach is uncomfortable. As a breast cancer survivor, wearing around my neck is also uncomfortable." – *anonymous*

Comfort is clearly a significant principal for this interface and the use of a facial detection system alleviates the primary concerns from survey respondents as well as the evaluation. Lastly, and thankfully, a majority of the respondents are inclined to allow a security system to maintain their facial data, which had been a privacy concern for this redesign consideration.

Transition from the key to the badge reduced the users gulf of execution, however, the facial detection system further reduces this gulf. The intentions of the user while executing the interface is still the same, they want to access a permitted area, but the actions needed to accomplish this task is greatly reduced. Users need not find their badge, remove it, put it against the scanner, and put it back to where it was taken, they simply have to look at the camera, and that is it. This reduction in the number of actions also further increases the ease of the system since their object of entry cannot be forgotten or misplaced. As a result of this simplification, cognitive fatigue surrounding the need to remember a badge as well as maintaining a mental awareness of its location throughout the instance is alleviated. Resulting from this reduction is an interface that progresses closer towards an invisible one the moment the user begins to interact with it.

In addition to the interface becoming more invisible, the facial detection redesign also improves the principal of direct manipulation for the user. For a user knowingly progressing towards a secure area that they have access to, they should feel in control of the situation and not be stopped by a system to verify their identity. Simply looking into a camera near the entry point and being provided access improves the manipulation of the locking mechanism for the door, since it almost feels like to the user that it is reading their mind.

In the modern age, cameras afford the property of being looked at. They are very perceptible to most people and usually distinguishable from its surroundings, making it a common object that people tend to be aware of. While this affordance is often negatively perceived in practice as a feeling of scrutiny and governance, in this situation, it encourages its intended use.

In addition to this affordance, maintaining the badge reader in the vicinity improves the user's mental model and mapping of the system by associating the functionality of the camera with it. With the user's mental model of knowing what and how the card reader works in relation to the door, ideally the user can map that understanding to the camera near it. Since the indicator light is shared between both systems, the user

should be more comfortable in the situation when the indicator turns green after looking at the camera, because they can map the new result with their previous understanding of the system. With these two principles and the addition of the signifier, it results in a very rapid learning curve. Minimal experience and interaction with the system is needed to reach proficiency, especially if a user has a strong mental model of the badge system.

Lastly, use of the camera system alleviates the need for multiple cards; the user only needs a single face. With 71% (22) of respondents reporting that they use multiple cards, and a majority of users stating that carrying even one is a hassle, this characteristic needs to be addressed. Utilizing a facial detection system inherently removes this flaw. Ideally, facial identification data can be transmitted from system to system which doesn't change based on the type of system being used, where different badge systems may require different badge technologies.

Implementation of a facial recognition system addresses both the criticisms identified in the evaluation section, as well as the voices of respondents from the survey. The major inconvenience and constraint of having to carry a badge is replaced with only needed the persons presence, and the inflexibility of badges at different locations is also similarly addressed. As an added justification, the survey has identified that the primary concern of holding a user's facial data is not a concern for the majority of respondents. With this redesign supplementing the badge system, users are accommodated with both systems if they happen to have a personal preference, or do not want to have their facial data stored.

References

1. Cardullo, Mario W, and William L Parks. *Transponder Apparatus and System*. 23 Jan. 1973.
2. Potts, Dan T. *Locky and Key in Ancient Mesopotamia*. XXV, Casa Editrice Le Lettere, 1990, pp. 185–192, *Locky and Key in Ancient Mesopotamia*.
3. Calistra, Cole. "Face Detection Explained." *Kairos*, Kairos, 22 Feb. 2015, www.kairos.com/blog/face-detection-explained.
4. Doshi, Keval. "Face Detection Using Raspberry Pi and Smartphone." *Hackster.io*, Hackster, 12 Sept. 2017, www.hackster.io/keval-doshi/face-detection-using-raspberry-pi-and-smartphone-19f1f2.

Appendices

Survey Questions:

Question Number	Question	Response options
1.	Do you or have you used a badge or access card to enter a physical area?	Yes/No
2.	Do you use more than one access card?	Yes/No
3.	How often do or did you use this type of security system?	All the time/ Rarely/ Never
4.	What do you dislike most about using an access card?	(Free response)
5.	Have you lost or forgotten your access card before?	Yes/No

6.	Do you find carrying an access card to be inconvenient?	Yes/No
7.	Would you be comfortable with a company holding your facial data for use in a security system to replace an access card?	Yes/No
8.	If not, why?	(Optional, free response)

Table 1: Survey questions and response options

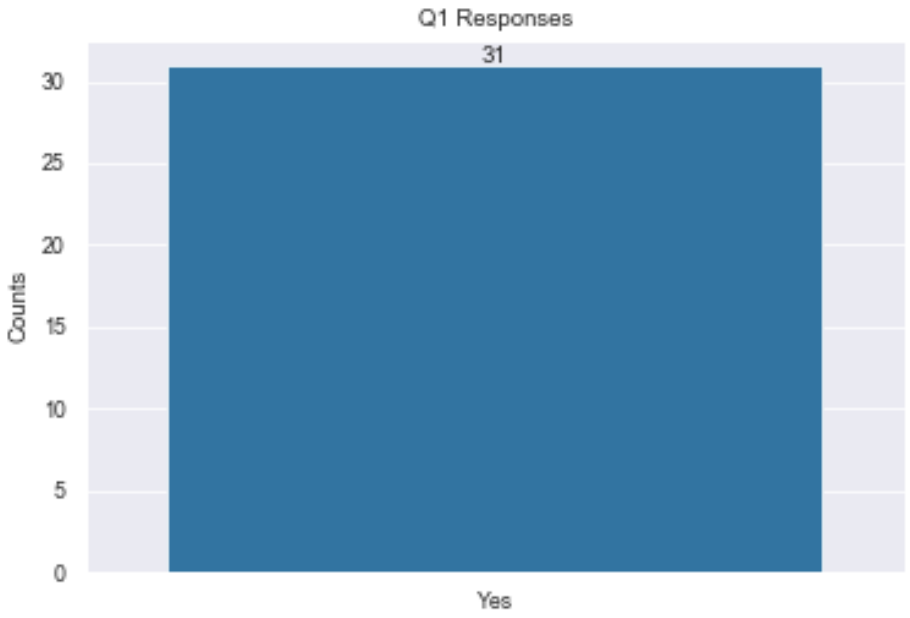

Figure 4: Question 1 responses

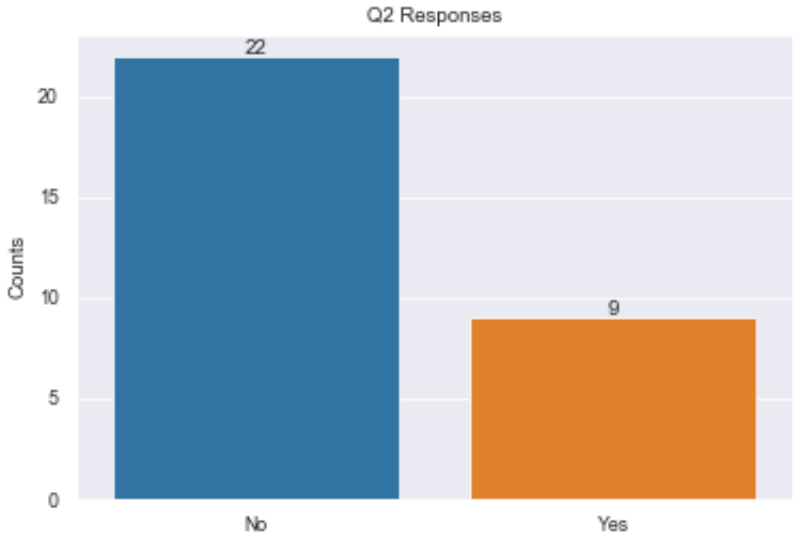

Figure 5: Question 2 responses

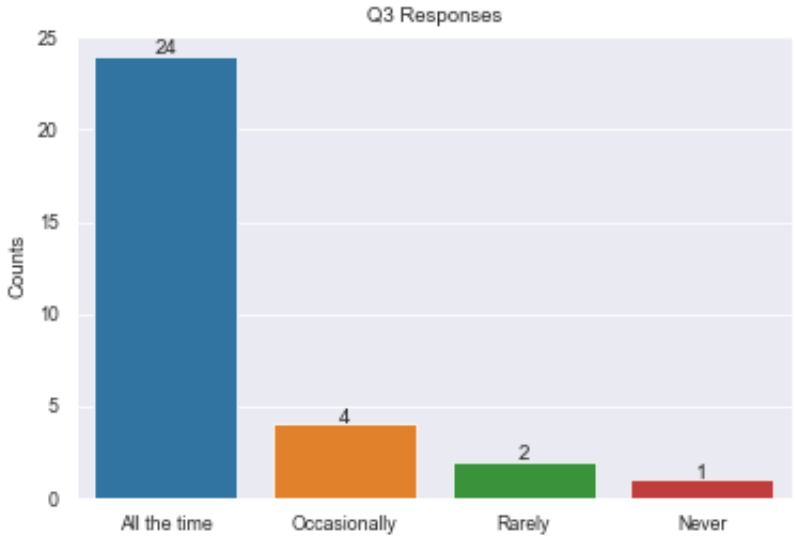

Figure 6: Question 3 responses

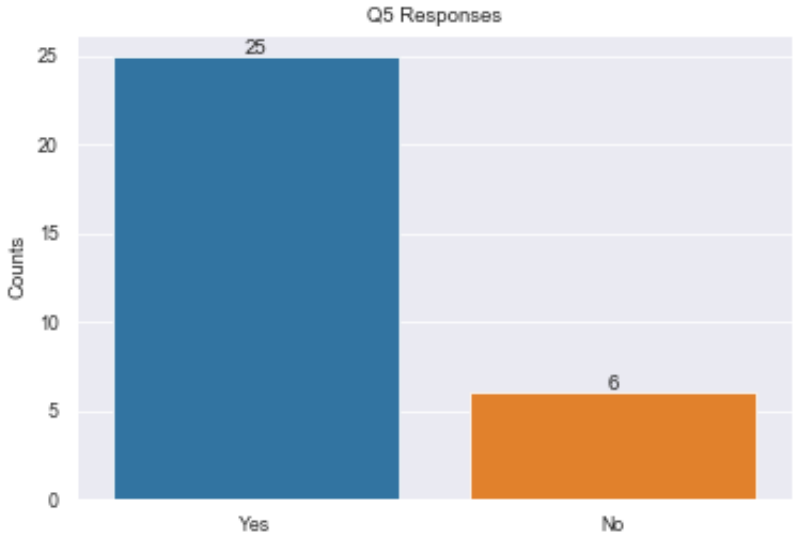

Figure 7: Question 5 responses

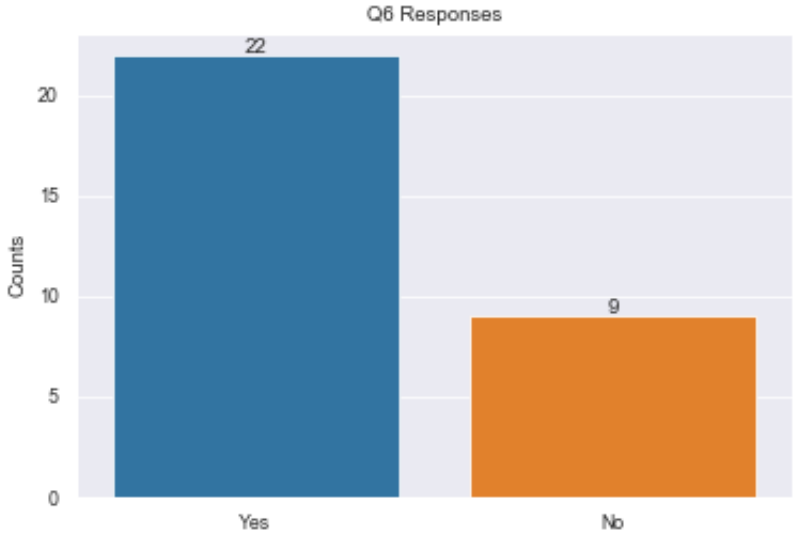

Figure 8: Question 6 responses

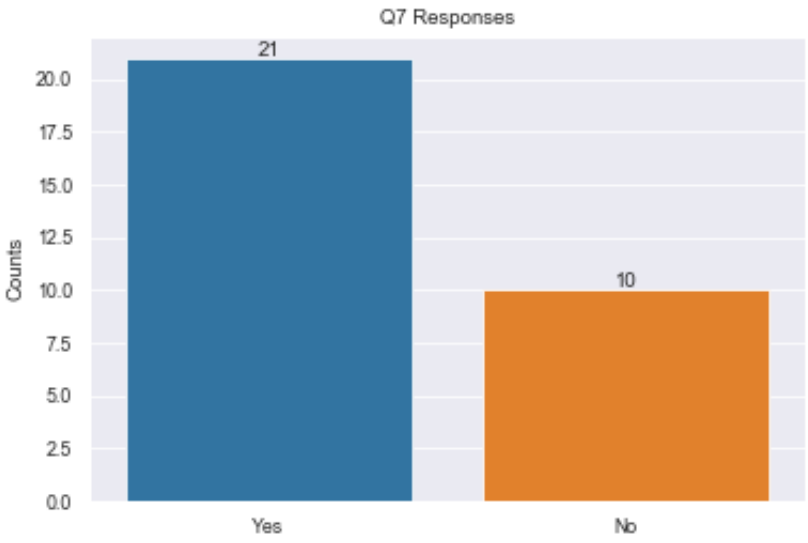

Figure 9: Question 7 responses