The surveillance university

Student’s name

Institution

**Introduction**

Surveillance is practice in the universities to provide a safe, secure and healthy environment for students, staff, and other stakeholders. According to Wilson and Wells (2017), the practice of surveillance is to ensure that crimes related activities within the university can be detected and prevented on time. A study conducted by Saha and Neogy (2014), pointed out that the issue of surveillance in the university must address privacy and confidentiality of stakeholders. This has made it difficult for institutions to conduct optimal trace of activities within a campus. However, it could be easier to monitor every student and other people within the university through the use of CCTV cameras, and facial recognition but this had to be done concerning the privacy of students and other members of the university. This report, therefore, provides a recommendation on what should be done to balance the security and privacy of students and other university members.

**Available Technologies**

For efficient monitoring and tracking of students to provide security, which can deter terrorism activities in the university, the university would have to consider the installation and implementing of face recognition, location tracking, phone monitoring, and CCT system throughout the campus and inside the classrooms. Each of these technologies operates uniquely and the applications of the technologies should be implemented concerning the rule of law observing the privacy and rights of students.

**Face recognition**

Face recognition is described as a high technology, which can identify or verify a person using digital images or videos. It utilizes biometric to map out features of a video or a photograph. According to (Omand, Bartlett, & Miller (2015), it compares the information in the database, with the image or video of a person being verified. Therefore, for it to be used efficiently for the verification of persons there must be a database whether from the government of private data. The use of facial recognition technology software will help the university to monitor every student within the campus in order to identify the suspected students working with terrorist organizations. The technology has been used by several organizations and governments and therefore, its application by the university would not be illegal if the law is followed appropriately. The use of government and mobile companies has used it for decades and therefore, it is the best technology, which can help the university to identify potential persons working with the terrorist group from Bangladesh.

**Phone monitoring**

Phone monitoring is one of the latest technologies used to monitor people. The phone monitoring technology tracks the mobile communication and text person of a targeted person. Its application has been challenged by several activities and other individuals. But it is the best option for the university to ensure that activities of every potential threat are properly monitored to prevent any potential attack on the university (Desai, 2017). The university needs to get a warrant to conduct the monitoring against the students to avoid any legal case. The act is not allowed to an extent by with warrant to detect potential terrorist activities, the university would be able to monitor phones of every student and this would help in getting all the information or communication of students when on campus and out. The institution would be able to listen to every detail of communication between students and other people through their mobile phones. It is pointed out that these students are from Bangladesh and they have a connection with the terrorist group back in Bangladesh. The using of mobile listening would be the best effective method to monitor the communication between the terrorist and the suspected students and this would be helpful in the identification of the said students.

**Location tracking**

Location tracking is one of the latest technologies used for tracking persons. It is used to identify the specific location of targeted individuals. Wilson & Wells (2017) pointed out that it used to point the whereabouts of strangers. It would be the best tool or technology for tracking the whereabouts of every individual within the university. It pinpoints the exact location of a person and therefore, it makes it easy to locate an individual. The location tracking used the global positioning system (GPS) to retrieve the position of an individual using mobile phone data. The university would be able to track every student using location tracking and this would allow the institution to detect and trace everyone in real-time.

**CCTV cameras**

Without the use of CCTV Camera, it is difficult to know whether and what an individual is going every minute when within the campus. Ideally, the installation of CCTV and the use of facial recognition software could provide the best level of monitoring activities in the university. Most researchers have pointed out that there are certain problems associated with the installation of CCTV and other surveillance activities in the universities and even in public places. According to Wilson and Wells (2017), the methodology used is difficult to conduct proper control evaluation. The information can be exposed and this could compromise the privacy of students. The use of facial recognition software and the monitoring of mobile phone communication are essential for securing university. But it is difficult to practice surveillance without violating the privacy of people. (Beaver, 2014) pointed out that though the security of students and other stakeholders in the university is crucial, the privacy of students is more students because it is part of students' rights which must be protected by the university.

**Monitoring Mechanism**

Monitoring activities going on within the university is an important aspect in improving the security of students. The issues related to terrorism are critical and cannot be treated lightly and therefore, having effective surveillance would be ideal. The use of a security checkpoint at every entry in the university would be the best idea in ensuring that every person walking into the university does not carry any harmful material. As stated by Kittle (2013) checkpoints introduce thin surveillance at every entry to make sure everyone in the university is accounted for. The checkpoint will allow the university to know several people in the university and when an individual walks in and out. It, therefore, improves the security and safety of students and other people in the university. The application of facial recognition and CCTV cameras and monitoring of mobile communication are good concepts that the university must consider to protect the university from any attack. Since the Homeland Security Department has singled out the university for likely to be attacked, it would be of importance for the university to monitor student's communication and moving to identify suspicious students. Though mobile monitoring cannot be allowed by students and it is illegal since it betrays individual right to privacy, the use of communication surveillance to trace suspicious students would be of great importance to the university. According to a study published by Perrino (2018), monitoring students' activities on and off-campus is critical for improving security. Most universities monitor students' behavior and movement when on campus to ensure the security of the university. This is an effective strategy that can help the university to monitor activities of students and therefore, it could help to identify radical students. Without close monitoring of students, it would be impossible to detect radicalized students and therefore, terrorism prevention would not be achieved.

Moreover, profiling students would be of great help to the university administration to narrow down suspicious students faster. But it would be a violation of university culture and norms. However, the university can deploy profiling based on the early signal of questionable activities by students. Profiling could be discriminatory and could put the university in a problem with the justice department (Bradley, 2017). However, evidential profiling would be welcomed. It is pointed out that some students from Bangladesh are working with organized groups to launch a terrorist attack in the university. It would be important for the university to identify students from Bangladesh and put them on serious surveillance (Desai, 2017). Security of student’s come first for effective provision of security it would be essential for the university to conduct profiling in order to get the suspected students from Bangladesh. The best option for the university is to seek a court warrant to permit surveillance on students and profiling as an option of conducting an investigation. The judge would be willing to issue a warrant for the security of the university.

Mobile monitoring would be rejected by students and other stakeholders for fear of violation of students' privacy. Implementation of the mobile monitoring concept through a secret method without any student realizing would be the best option for the university to spy on every student without anyone knowing. (Dans, 2018) pointed out that the federal government spy on people every day using different software and hardware and the practice has been used for decades. The National Security Agency (NSA) stated that the use of spy software and monitoring mobile phones of people randomly practiced in the United States to prevent the country from imminent attack (Petterson, 2015). According to a report by the NSA, several attacks have been prevented due to the use of spy software and mobile monitoring technologies. Therefore, this practice can be adopted by the university and practice in secret to provide maximum security to students.

**Advantage**

The establishment of surveillance within the university has been used by several universities in the United States and it is a permitted practice by law. However, one major advantage of practice would be the improved security of students, staff, and visitors. The institution would be able to detect and prevent any act of criminality and therefore, a secure environment for earning would be established. The use of surveillance technology allows the institution to monitor every student and therefore, tracking and monitoring events in the university would be easy. Tracking and arresting anyone trrying to commit crime wouold be faster and easy and therefore, any act of terrorism would be prevented.

**Constraints**

The use of surveillance technologies violates the right of the public. It is highly likely that the privacy and rights of students would be violated. According to Wells & Miller (2017), the violation of the privacy of the public including students can lead to illegal battles. Therefore, the installation and use of surveillance within the university can result in legal suit from students against the administration. It caused the university a lot of legal compensation due to violation of privacy which is against the cybersecurity and privacy law of the university. It is also difficult to convince students of the importance of surveillance. The majority of students will likely reject the idea to provide their mobile details and other information which can allow the administration of the university to monitor and track. This is likely to affect the result and efficiency of the process.

**Recommendation**

It is recommended for the university to install CCTV cameras in every classroom and in the entire university as the first action to ensure that the students and other staff are protected. Though profiling of students is against norms and culture of the university and it is also illegal and discriminatory, the activation of profiling of students based on their original would be an option. Profiling helps in gathering data by narrowing the target to specific people rather than focusing on over ten thousand students. The university administration should investigate a partnership with the local police to identify the students who can be the culprit. Without profiling and working with the local police it would be difficult to track down a suspect which has been identified as students from Bangladesh. It is also recommended to use an internet platform to monitor students' activities online. The university should use its network infrastructure to monitor everything which students do online. The use of spy software to monitor students’ activities on Facebook and other social media would help in the prevention of attacks in the university. All these activities should be done within the framework of the law to prevent violation of the students’ rights (Wells & Miller, 2017). To ensure that the privacy of students is not abused and the monitoring system set up is not misused, it would be essential for the university to have strict policies and regulations regarding the use of the system to ensure that students' information is not shared with the public. All the stakeholders would be required to come together to have an effective debate and to agree on the formula to use in monitoring students.

**Conclusion**

Balancing security and privacy is a challenge to administrations and government. For the university to conduct surveillance on students there must be appropriate regulations and policy to have such a system in the university. It is established that the use of CCTV, facial recognition software and profiling would be an ideal strategy to track and get suspected terrorists from Bangladesh. Therefore, the university needs to work the judicial or the justice department to get a warrant permitting it to conduct profiling, mobile monitoring, and other surveillance activities to protect students from any kind of attack. The university should create a back entry into students' phones for any student using a university's WIFI internet connection. Studies have indicated that most students use free wifi and LAN internet connection within the campus (Omand, Bartlett, & Miller, 2015). This makes it easier for the administration to create a back entry, which can be used to monitor students' communication when on campus. The facial recognition software should be used to identify people within the campus to help to track the movement of everyone (McCaine, 2018). The use of facial recognition would help trace, to know where every student is doing every time and also to collect data related to friends and associates of students. Gathering this information will help the university to provide effective monitoring of students, which is critical for the security of students and the university in general. All students should be subjected to monitoring and the narrowing down to one or a few groups of students should be done based on the analyzed data gathered during the process.

# References

Beaver, K. (2014). Information privacy and security requires a balancing act. *International*

*Journal of Information security*, 2-17.

Bradley, T. (2017). Finding The Right Balance Between Security And Privacy. *International*

*Journal of information security*, 2-15.

Dans, E. (2018). Surveillance In Schools: Where Is This Taking Us?

*https://www.forbes.com/sites/enriquedans/2018/08/23/surveillance-in-schools-where-is-this-taking-us/#43319063bee7*, 2-15.

Desai, N. (2017). Balance privacy and Security in digital agae.

*https://policyoptions.irpp.org/magazines/july-2017/balancing-privacy-and-security-in-t he-digital-age/* , 2-15.

Kittle, J. T. (2013). A Study of Surveillance and Privacy Rights. *Electronic Theses and*

*Dissertations. Paper 1170.* , 2-15.

McCaine, M. (2018). Information privacy and security requires a balancing act. *Journal of*

*Information science and security, 21* (43), 1-25.

Omand, D., Bartlett, J., & Miller, C. (2015). A balance between security and privacy online must

be struck. *Journal of National Security*, 14-35.

Petterson, P. (2015). National Security Agency: Security and Privacy Analysis. *Journal of*

*national security and technology*, 2-15.

Saha, S., & Neogy, S. (2014). A case study on smart surveillance application systems using WSN

and IP webcam. *Applications and Innovations in Mobile Computing (AIMoC)* , 12-38.

Wells, S., & Miller, C. (2017). Balancing Security and Privacy in the Digital Workplace. *Journal*

*of Change Management*, 2-34.

Wilson, P., & Wells, H. (2017). What do the watchers watch? an Australian case study of CCTV

monitoring. *https://pdfs.semanticscholar.org/1fdf/795da1bd7643e54beee954f7d5f0776ec43f.pdf*, 2-15.