The University of Hawklandia is facing an exciting decision of whether to implement facial recognition technology onto our campus. As the President of this Big 10 institution, home to 30,000 students, I have taken the time to construct my decision on the matter with utmost consideration of the options, shareholders, and stakeholders. FaceTech has approached us with proposals they suggest will "pay for themselves" with the monetary benefits they offer through customer convenience. At Herky Football Stadium, the facial recognition software will identify malefactors, facilitate student purchases, and regulate the sale of alcohol. In addition, we have the option to incorporate the technology on the rest of campus for accurate class attendance and, potentially, the tracking of students across campus security cameras. While there are many perceived monetary and convenience benefits, ethical considerations may sway us to consider our final option, which is to reject the implementation of facial recognition technologies on our campus altogether. After deliberation with the use of ethical frameworks, I have come to the decision that our university should not implement facial recognition technology in the interests of student privacy and the reputation of our university.

All four of Joseph Badaracco's frameworks for decision making offer good points to think about while reviewing the scenario. The first framework describes how one should pick a decision that does the most good and least harm, in a term Badaracco coins the "best net-net consequences". Badaracco's second framework describes how one should consider the rights of involved parties that cannot be violated under any circumstance. The third framework warns that whatever decision one makes will send a message to the world about one's ideals and rights, so one must think carefully about what one's actions say to others. Badaracco's fourth, and final, framework states that decisions must be reasonable and consider what will actually work in the

world today. While I could make cases for all four of Badaracco's decision-making frameworks

to apply, I think frameworks two and three provide the most pertinent considerations for this

decision, and therefore I will use those two to justify my recommendation of not implementing

facial recognition technology in our stadium or on our campus.

Each person possesses uninfringeable human rights, and it is internationally agreed that

privacy is one of those rights. The United Nations' Human Rights Council consistently revises

their articles on the right to privacy in the digital age. In relevance to Hawklandia, they

acknowledge that automated processes and transactions can affect individuals' privacy, and that

any non-essential interference with a person's privacy should be avoided by both states and

business enterprises (United Nations Human Rights Council, 48/4). More specifically in the

United States, several individual states jurisdictions have enacted laws prohibiting and restricting

law enforcement's use of facial recognition technology (Lively). If even law enforcement faces

backlash towards its use of facial recognition technology, Hawklandia would almost certainly

face backlash as well. If we use technology to create data identities of each student containing

biometric data, it could be a violation of students' privacy and a violation of their uninfringeable

rights.

One could challenge this idea with the possibility that students do not think of it as a

violation of their privacy. Though we cannot read the minds of the public, there is evidence

customers would not be comfortable with us having this data. Nature, an international science

and technology publishing group, took a survey of 500 researchers in the realm of facial

recognition technology on their opinions on the matter, and over 60% of participants said they

would be extremely uncomfortable with "companies tracking people in public spaces" and

"schools assessing student's behavior" (Van Noorden). As researchers in the field, one would expect this crowd to be the most enthusiastic about implementing this technology for the furtherment of their own careers, and yet only about 10% were actually comfortable with either of these practices (Van Noorden). In the rural-dominated state in which the University of Hawklandia exists, most of the population would be far less enthusiastic than these researchers when it comes to the collection of personal data, and therefore we can assume most people at our football games and on our campus would be extremely uncomfortable with these practices as well.

After the students decide whether their privacy is violated, they lead to the next ethical framework, where the students, and world, construct a narrative of our university's values based on our actions. The refined identification of malefactors could improve student safety and become a positive narrative formed from using facial recognition technology; however, the rarity of malefactor scenarios means the larger population will only see the function of using it for student purchases. If the majority of students see the main benefit of this technology as convenience for purchase from the university, they will instead form a negative perception that Hawklandia values profit over consumer privacy. As a university of over 30,000 students, we already implement extensive marketing and frameworks to make our university appear and feel more intimate and our students feel cared about. If we take profit over people, we align ourselves with large corporations who would do the same, and in turn, we erase our progress toward community on our diverse campus.

And on the subject of diversity, our university could take heat if FaceTech's technology shows any form of racial bias. Racial biases are a prevalent issue with facial recognition technology because these programs must be specifically trained to distinguish the smallest

discrepancies in each ethnicity or race. Though strides in accuracy have certainly been made, "a

growing body of research exposes divergent error rates across demographic groups, with the

poorest accuracy consistently found in subjects who are female, Black, and 18-30 years old"

(Najibi). This age range perfectly encapsulates the ages of the average university student.

According to the same study, "error rates [for dark-skinned females were] up to 34% higher than

for lighter-skinned males" (Najibi). High error rates lead to misidentification of targeted groups,

and therefore create mistreatment through wrongful conviction. This disparity makes the

technology a morally wrong implementation, one that would be egregious to use in the

identification of malefactors. Misidentification could turn into a huge scandal for the university

as we will be exhibiting racist behavior. Because the technology cannot be trusted to identify

people of all appearances accurately, we cannot use it to enforce serious protocols. Besides, we

should be able to monitor students well enough by matching students to their student IDs before

letting them into the stadium. If we choose to implement facial recognition technology, we

display values of greed and potentially racism.

In conclusion, I recommend abstaining from implementing facial recognition technology

onto our campus. While it would be highly convenient for the students who consent to use it and

raise revenue, there are ethical concerns for privacy, the rights of students, and the accuracy of

the technology. Badaracco's second framework brings a wise consideration for the

uninfringeable rights of man, and, in the US, it has been proven in courts that privacy is one of

those rights. Based on field studies and the climate of the state our university is in, we can

assume the student body would share this viewpoint. With Badaracco's third framework in mind,

one that says our actions are a message of our values, I have concluded that infringing on student

privacy in the interest of profit and convenience will align our university with the image of a

large, greedy corporation, one who values efficiency over the livelihoods of its employees. This will ruin the image of community we are trying to build. And so, although FaceTech's proposal would bring efficiency, this is a time where we have to value our students over the machine.

Works Cited

"Chapter 22: The Right of Privacy." *Annenberg Classroom*, Annenberg Classroom, 9 Oct. 2018, https://www.annenbergclassroom.org/resource/our-rights/rights-chapter-22-right-privacy/.

Hoffman, David. "Privacy Is a Business Opportunity." *Harvard Business Review*, Harvard Business Review, 2 Nov. 2014, https://hbr.org/2014/04/privacy-is-a-business-opportunity.

Lively, Taylor Kay. "Facial Recognition in the US: Privacy Concerns and Legal Developments." *ASIS*, ASIS International, 1 Dec. 2021, https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/.

Van Noorden, Richard. "The Ethical Questions That Haunt Facial-Recognition Research." *Nature News*, Nature Publishing Group, 18 Nov. 2020, https://www.nature.com/articles/d41586-020-03187-3.

United Nations General Assembly. *Resolution adopted by the Human Rights Council on 7 October 2021,* A/HRC/RES/48/4, available from undocs.org/en/A/HRC/RES/48/4