

Technology Unmasked: The Argument Against Facial Recognition Technology

Lisa Luong

As one of the best universities in the nation, the University of Hawklandia prides itself on the students it produces, the staff it hires, and the state it represents. With over 30,000 in attendance, decisions are taken into much consideration to ensure the very best for our students. In addition, we recognize the impact of the decisions we make on our staff, the Big Ten conference, alumni, donors, and other partners. Therefore, the recent proposal in using facial recognition technology by FaceTech is not to be carelessly decided upon. After extensive evaluation with help from the university's legal counsel, as well as other outside sources and research, a definitive conclusion has been made on the proposal. As President of the University of Hawklandia, I recognize the growth of collegiate sporting events and the need for better security at such events to protect those in attendance. However, I have decided against the use of all facial recognition technology proposed by FaceTech because of the safety concerns over data access and storage, the privacy concerns over personal information, and the risks of technological profiling and biases.

I came to this conclusion with help from Badaracco's four frameworks for a decision. The first is net-net consequence. It lists out everyone affected by the decision, and one must decide who is to be prioritized. The second is the individual rights of individuals or groups that cannot be violated due to the decision. The third is character meaning what do you and your organization stand for and the impact on integrity of the decision. And the final framework pertains to what decision will work best in the world as it currently is. The proposal given before me includes a system developed by FaceTech with the capacity to store photos and recognize the faces of all students in attendance through student ID photos and other information. It would help

enforce bans, purchasing of concessions by facial scans, and preventing illegal alcohol purchases by students at Herky Football Stadium. The proposal also contains add-on options to take attendance of students in classrooms through facial recognition as well as automatically identifying students who appear on existing campus security cameras. Using three of the four Badaracco frameworks, I will discuss my decision against the implementation of FaceTech's technology proposal at the University of Hawklândia.

To begin, the safety of our students is top priority at the University of Hawklândia and it is our responsibility to ensure student information is safe. The safety concerns regarding FaceTech's proposal is how the facial recognition data is to be stored and accessed. With all technology there is risk of it being hacked and the data stored being stolen. For instance, a US Government agency had its data breached, "In 2019, more than 100,000 photos and license plates were stolen from the Border Agency database" (Fox, 2020). If the US government can be breached it is without a doubt FaceTech can be breached as well. The risks of personal data being stolen is much greater than the potential for more efficient security measures. Using Badaracco's first framework on net-net consequence these are risks our university will not take. The proposal will not only affect our students and staff, but all those entering in and out of the stadium. To add, FaceTech argues that increased revenue from food and beverage sales alone will be sufficient to pay for the technology. However, the money made from concessions is not a consistent source of funds and therefore cannot be relied upon due to varying attendances and concession sales at all games. Our university would rather commit funds to other security measures as opposed to FaceTech's senseless claim of the technology paying for itself. There are many ways to invest money in more efficient security that does not require sensitive data like hiring additional guards, specialized people to enforce bans and detect illegal alcohol purchases,

and advanced metal detectors. To reiterate, our priority is the safety of our students as well as those we host at our sporting events. The university's position is firm in rejecting FaceTech's proposal to ensure no unintentional effects occur and put those we are responsible for at risk.

Next, privacy is another concern regarding students' individual rights as personal information in official university records would be used. The proposal goes beyond using photo IDs at entrances into the stadium by using students' birthdates in official university records. This is to identify those illegally purchasing alcohol during games. Though this is a concern for any university at any sporting event, the use of personal information to identify students' age outside of academics without consent is a reckless overreach in our authority. Official university records should not be casually distributed. In addition, people have altered their appearances to trick similar technology, therefore making it useless, "he has confused facial-recognition software into thinking he was someone else by wearing specially designed glasses or Band-Aids" (Olson, 2021). Using Badaracco's second framework on individual rights, we considered the privacy of all those entering Herky Football Stadium during the games. These people include, but are not limited to, students, fans, faculty, medics, security guards, and media personnel. A key goal in the proposal is to prevent underaged drinking by students, but FaceTech does not consider non-students who purchase alcohol underaged during games. The university can only provide information of students currently in attendance. There will be no way for FaceTech's technology to flag those who are underaged but not affiliated with our institution from purchasing alcohol. To add, those over the age of 21 could purchase alcohol for underaged students during games and not be flagged as well. Therefore, personal information of non-students must also be collected for this goal to succeed. As President, I cannot implement the proposal as the university would not only violate the privacy of students, but all those entering the stadium by providing

and requiring such personal information to maximize FaceTech's effectiveness.

The final issue is the accuracy of the technology proposed by FaceTech in detecting individuals. Sports has always been a way for people to come together and put differences aside to support a team. In today's social climate, it is essential for all our students to feel safe and accepted at all university sporting events. Facial recognition technology is not free from prejudicial profiling and biases, "A recent report by the National Institute of Standards and Technology studied 189 facial recognition algorithms which is considered the 'majority of the industry.' The report found that most of the algorithms exhibit bias by falsely identifying Asian and Black faces 10 to beyond 100 times more than White faces. Moreover, false positives are significantly more common in women than men, and more elevated in elderly and children, than middle-aged adults" (Jackson Lewis P.C., 2021). This type of technology is not free from errors and the risks of inaccurately identifying individuals is a real possibility. Using Badaracco's third framework on character, any kind of profiling is not what the University of Hawklandia represents. It is important that all students at our institution feel safe and accepted as well as those attending our sporting events. Furthermore, inaccurate profiling could lead to decreased revenue from games and a stain on the university's character. The character of this institution not only represents those currently in attendance, but sets a standard for what we believe in to those worldwide, inaccurate profiling of any kind should not be acceptable. To restate, the university will not commit to FaceTech's proposal. The technology proposed is not foolproof and inaccuracy is bound to occur. As a leading academic institution, wrongful profiling of those attending sporting events is not what we want to be known for.

To conclude, as President of the University of Hawklandia, I have decided not to implement FaceTech's technology proposal in its entirety. This is due to safety concerns of data

breach and manipulation, privacy concerns of students' information for use outside of academics, and risks of profiling and inaccuracy. Data is always at risk of hacking by outside sources and a person's appearance is never guaranteed to stay the same. The use of personal information to track student activity is an unnecessary overreach in our authority. And finally, the potential to inaccurately identify and profile individuals is not admissible to the university's principles. After using three of Badaracco's frameworks, it is clear the use of facial recognition technology would be irresponsible. As technology continues to advance every day, there must be an understanding of the new risks associated with it. Through the denial of FaceTech's proposal, the university's commitment to ensuring the very best for our students remains firm. Our students are the future teachers, doctors, lawyers, politicians, and businessmen and women of this next generation, and at the University of Hawklandia, we dedicate ourselves to their success.

References

- Badaracco, J. (2003). *Defining Moments: A Framework for Moral Decisions*. Harvard Business School Publishing Class Lecture. <https://www.hbs.edu/faculty/Pages/item.aspx?num=15483>
- Fox, H. (2020, October 1). *3 Privacy Concerns Around Facial Recognition Technology*. Swiftlane. <https://www.swiftlane.com/blog/facial-recognition-privacy-concerns/>
- Jackson Lewis P.C. (2021, July 28). *As Facial Recognition Technology Surges, Organizations Face Privacy and Cybersecurity Concerns, and Fraud*. The National Law Review. <https://www.natlawreview.com/article/facial-recognition-technology-surges-organizations-face-privacy-and-cybersecurity>
- Olson, P. (2021, July 7). Faces Are the Next Target for Fraudsters. *Wall Street Journal*. <https://www.wsj.com/articles/faces-are-the-next-target-for-fraudsters-11625662828>