

Flavio Cervantes

CST300-30_2252

February 19, 2025

Facial Recognition is Everywhere

Introduction/Background

Private businesses must protect their assets, no matter what the cost to their consumers privacy will entail. Facial recognition (FR) utilizes intelligent video streaming technology, database queries, efficient processing and many more components operate in conjunction to achieve capturing video streaming data, which is then analyzed and interprets their patron's identification. This is important data because a business can leverage this data for finding missing patrons, operations efficiency, contactless transactions, and heightened security. (Erika, 2024) One may argue that private business should not be able to utilize facial recognition because one runs the risk of getting flagged as false-positive, hence getting unwanted attention, or running the risk of randomly getting arrested, uncertainty of data privacy compliance. Lastly private business' do not have signed consent to capture personal FR data.

FR development started over fifty years ago, at first it was not successful due to factors such as head movements, lighting, facial expressions, and aging. Thanks to improvements with camera technology, machine learning, faster and efficient processing we are now able to rely heavily on accurate FR. (Thales, n.d.) This provides important benefits such as private businesses are now able to protect their assets in a proactive approach. This valuable technology has changed the dynamic of surveillance departments tremendously by improving efficiency, patrons experience and also operational efficiency. Day-to-day task can leverage the technology

FR provides to save time consuming manual task such as back-tracing one's steps for potential criminal investigations.

This became an issue for various reasons such as the utilization of facial recognition to protect their assets, but one can argue that private entities should not be able to use FR because of inaccuracy, risking privacy data leak which can cause exploitation, & biometric vulnerabilities. Ethical frameworks also raise concerns with FR due the rights of the individual and not obtaining consent.

Stakeholder Analysis

Pro stakeholder would argue that the benefits of FR are related to the ethical framework created by Immanuel Kant, which is the Kantian Deontology. This framework expresses the importance of morality and benefits that FR can provide, and how human values and rights are not compromised due to the privacy protection, universal security laws such as having good behavior in public places. Con Stakeholder counter argument on why FR should not be utilized without consent, privacy related ethical frameworks support the argument that consent should be granted before collecting unnecessary data. Private entities much hold accountability for obtaining consent due to privacy ethics. Integrity and confidentiality can be misused since there is no guarantee that FR data is being collected for the respective purpose.

Stakeholder 1

Data Security Frameworks is another ethical framework that supports the “pro stakeholders” position. This framework was developed by the cyber security specialists in order to regulate and ensure data privacy.

FR should be utilized without consent in a private business because it assists in day-to-day business operations by leveraging pro-active approaches when enforcing keeping certain banned patrons out. By utilizing technologies such as license plate readers combined with facial recognition, businesses are able to detect blacklisted patrons from the time their vehicle gets flagged through the cameras software and notifies operations. This attracts attention to this certain individual; hence they will be able to leverage facial recognition once they walk past a respective camera and have technology confirm that it is a positive match. This avoids human interaction from being a culprit in a possible false positive or false negative.

It can also be utilized to keep track of number of patrons for data analytics purposes. By keeping track of busy areas and comparing those analytics to desolated areas, marketing specialist can determine to add certain entertainment attractions to the desolate areas to try to improve walking traffic flow to that certain area to boost sales and revenue. By increasing the revenue that private entities are producing, they are able to output the income needed to keep investing into the architecture, hardware, and software development that FR systems utilize.

As a business owner, they should be able to know everyone who arrives and depart one's property. By leveraging FR one can accurately identify new patrons, VIPs such as loyal patrons, blacklisted players dressing up in incognito clothes, self-excluded players, merchants, state inspectors & Tribal members. (eConnect, n.d.) This data is critical to a business success because one can respond appropriately for each scenario. For example, if a tribal member arrives to the property, one wants to make sure that there is a dedicate surveillance agent keeping tabs to ensure their safety. The value this brings to the table is immense, since VIP patrons interchange a great deal of currency in the establishment. By ensuring they are content with business, it will

ensure they are satisfying with the establishment and keep them coming back to gladly continue spending their income.

Stakeholder 2

Universal Consequentialist Framework is the respective ethical frameworks that supports the “against stakeholders” position. This framework expresses the importance on equal consequences for everyone, rather than the individuals’ rights. This benefits the majority because widely held patrons do not have bad intentions, hence should not be at fault of the mistakes of individuals that have been blacklisted.

FR should not be allowed without ones consent due to the inability to ensure that one’s data is kept private. FR data is extremely sensitive information in this era, this type of data is more valuable than ever. External parties might utilize this information if exploited maliciously. (Erika, 2024) With respect to Utilitarianism, one can argue that the well-being for the majority of patrons is protected by not allowing FR, this will ensure that they are not at risk for a data breach due to visiting a certain private business that utilizes FR and is not practicing strict compliance policies or that has been compromised via a malicious attack.

The course of action of not allowing facial recognition without consent is the correct course because of privacy concerns, inaccurate screenings, invasion of privacy that may cause discomfort, malicious vulnerabilities and exploitations. (Erika, 2024). Privacy concerns raise concerns due to the collection of one’s biometric data without consent. Inaccurate screening is also another reason to why FR should not be utilized without consent, certain races and age groups are more difficult to determine, this can inadvertently cause a negative experience for an innocent patron that gets flagged as a blacklisted patron and has to prove oneself to security that

they are not blacklisted to continue their business at the establishment. By having constant video surveillance, one can feel uncomfortable since they feel as if they are always being watched, therefore cause unnecessary anxiety and stress due to cameras installed strategically for FR usages.

Argument Question

With respect to the overall-wellbeing of the people, should FR be allowed without consent?

Stakeholder 1

Private entities should be able to utilize FR since an influx of patrons can arrive at once. It is inefficient to hire humans to keep track of whitelisted or blacklisted patrons. Instead, FR can be leveraged to assist business operations in proactively keeping the banned patrons out, before potentially causing a massive problem. The ethical framework this relates to is “the common good”, the reason for this is because facial recognition keeps everyone safe, it helps casinos be pro-active on their uncertain approaches, rather than risking the satisfaction of innocent bystanders.

Stakeholder 2

This raises the concerns of having facial data exploited by cyber criminals that maliciously attacked an environment and now has hundreds of thousands or millions of FR images to use at their own will. These attacks can be spoofing attacks, reverse-engineering attack towards extracting sensitive personal information, adversarial attacks, which can be utilized to unlocks one’s cellphone via biometric authentication. (Chaintech Network, 2023).

This is a positive outcome for the stakeholder because it will minimize the risk of patrons getting flagged as false-positive, hence getting unwanted attention. In a worst-case scenario event, this situation would result in getting arbitrarily arrested. They should not be able to utilize FR without is because one does not know where the data is stored, and if gets compromised; one can run the risk of having one's facial image leaked on the internet for malicious purposes.

Student Position

Capturing this data has benefits such as leveraging business operations by keeping banned patrons out, assisting in having security be pro-active on uncertain approaches rather than risking the satisfaction of innocent bystanders. It can also keep track of patrons walking pattern to analyze busy areas or desolate areas. It can also be utilized to analyze patrons' steps in case of an investigation. FR should be used to protect a company's asset since private businesses are entitled to having surveillance system including facial recognition on their property.

This position aligns with that of the stake holders, it supports the positive aspects of private business enabling facial recognition without patron's consent. Due to the over-all wellbeing of their patrons, it is beset to utilize the technology that FR offers to maximize employee efficiency to have them perform more important task that can be automated via machine learning, video streaming technology, complex algorithms, etc. It is also very inefficient to have humans perform facial recognition. If one compares the speed of FR being performed through compute technology, one will realize that the human eye cannot compete with the efficiency computers are compiling the components needed to achieve FR.

FR is also able to track foot traffic that is coming inside/leaving the venue. It is an efficient tool for keeping track of how many patrons an establishment attracts in a day. Which can be used for

data analytics Determine the risk or financial gain factors, by tracking patrons accordingly. Back tracking patrons for potential criminal investigations, faster response times for critical situations, tailored customer service as certain patrons arrive at the establishment. (eConnect, n.d.)

A recommendation to solve the issue is to have city compliance enforce signs stating that facial recognition is being utilized in the respective business, and for any information or inquiries to reach out to a support number or website. This is the best course of action because private establishments will continue to protect their valuable assets, maintain a safe overall wellbeing of patrons, traffic flow analytics, and ensure important patrons are addressed according to best practices. This will ensure that privacy related ethical frameworks are respected and are being followed accordingly. By following best practices, it will ensure that patrons are comfortable interchanging their money in the respective establishment by having peace of mind that privacy and compliance laws are being followed. From a business owner perspective, it provides insight in daily day to day operations such as marketing analytics, efficient operations, and critical decision-making data that can be leveraged strategically to improve the establishment's weak-points.

References

Chaintech Network. (2023, November 17). *How Vulnerable Are Facial Recognition Systems to Attacks?*

Medium. <https://medium.com/@chaintech-network/how-vulnerable-are-facial-recognition-systems-to-attacks-c4d750c54e94>

eConnect. (n.d.). *eConnect | Facial Recognition*. [Www.econnectglobal.com](http://www.econnectglobal.com).

<https://www.econnectglobal.com/pillar-facial-recognition>

Erika. (2024, March 19). *Facial Recognition Pros and Cons: All You Need to Know*.

<https://www.deepseadev.com/en/blog/facial-recognition-pros-and-cons/>.

Thales. (n.d.). *Facial recognition history*. [Www.thalesgroup.com](http://www.thalesgroup.com).

<https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition>