Project and Professionalism

(6CS007)

A1: Professionalism Report

Facial Recognition Based Attendance System

Student Id : 2050058

Student Name : Ankit Tamrakar

Group : L6CG8

Supervisor : Ganesh Kuikel

Cohort : 5

Submitted on : 27-04-2022

Introduction

Professionalism can be multidimensional, as combination of assessment of various aspects are required. The proposed facial recognition system mainly deals with ethical and privacy issues as the data involved is highly sensitive and of great concern to the people involved.

1. Beneficial impact

The system has the potential to be beneficial by reducing manual workloads and carrying out every day's repetitive task in automation.

1.1 Attendance monitoring

Maintaining attendance is very important and compulsory in every institute and organization. Most organizations utilize traditional method of paper based or semi-automatic approach which is manual and time consuming. Handling and tracking attendance of large mass of people is very tedious and prone to manual errors.

Once facial recognition system is set up, it can be used for a variety of tasks, including attendance, lunch payment, and mood recognition. It may result in a reduction in the amount of manpower required, but it also increases the risk of failing to recognize students' needs and coming to terms with their human behavior. While automated data gathering systems may offer benefits in terms of speed, efficiency, and personalization, there is also the risk of overlooking essential form of socialization which is an important component of the learning process. (Andrejevic & Selwyn, 2020)

1.2 Finding missing people/belongings

When people go missing, there is only a certain amount of time to find them before the chances of finding them decrease dramatically. Many investigations begin by following the person's actions as closely as possible to the moment of their disappearance.

Surveillance cameras, when combined with facial recognition software to locate and monitor the person across a network of cameras, could be quite successful.

1.3 Security

Can be used to prevent school shootings, use of anomaly detection such as gun shaped objects and suspected criminals.

1.4 Validation of purchases

Proof of identification and verification such as ATM, ID cards, badges, passwords, etc. can easily be replaced by facial recognition. People can access their belongings, services, and devices without keeping track of keys or combinations.

2. Detrimental impact

2.1 Accuracy

One of the biggest concerns with facial recognition technologies is racial bias. Even though facial recognition algorithms guarantee classification accuracy of above 90%, these results are not universal. It's concerning that face recognition system faults were more common on dark-skinned faces, but there were less errors when light-skinned faces were matched.

The National Institute of Standards and Technology (NIST) conducted independent assessments in July 2020 to verify these findings. Facial recognition algorithms for 189 algorithms were found to have racial prejudice against women of color, according to the analysis. NIST also found that over half of the time, even the greatest facial recognition systems couldn't correctly identify a mask-wearing person.

2.2 Data breaches and ineffective legal support

Both the public and the government may have major privacy concerns because of data breaches. Breakthroughs in cybersecurity and growing use of cloud-based storage have resulted in the data becoming vulnerable to hackers, increasing the risk of Face ID theft in serious crimes. Victims of identity theft, have fewer legal options than other types of crimes. Data saved in the cloud can be secured against unwanted usage by adding an extra layer of security, such as encryption.

2.3 Elimination of obscurity and Increased authority

The aim is to leverage the fear of being caught doing the wrong thing at the wrong moment to make everyone behave in a certain way by always having cameras on. Rather than assisting in the capture of wrongdoers, this aids in the enforcement of social conformity. One of the most significant advantages of privacy is that people can do anything they want, whenever they want, if they are not breaking the law. The privilege is no longer available due to FRT.

2.4 Lack of informed consent and transparency

Researchers do not have a legal basis to gather images of people's faces for biometric study without their agreement under the EU General Data Protection Regulation (GDPR).

3. Ethical issues

3.1 Invasion of Privacy

The most common public concern is privacy. Citizens' fundamental right is violated by facial recognition and constant monitoring without their agreement. People’s lives are intruded upon. This could lead to false allegations and people altering the ways of living and going by their life. Installing facial recognition systems in public places, monitoring everyone from potential terrorists to every law-abiding citizen, results in an enormously intrusive force in people's life. Once a person leaves their home, their privacy is lost. People will have to be cautious about who they associate with and where they spend their free time, and they may even avoid going out in public because they are afraid of being watched.

What if, a person had to give up his or her right to privacy in almost all the public places, to live in a safer and secure country? This would imply that even the smallest of activities would be monitored and recorded to prevent malicious activity. Facial recognition revolves around a simple debate: privacy vs security. Although it has immense potential, it begs the question of whether facial recognition technology's lack of privacy reigns supreme and prevents people's lives from being their own.

FRT databases compile vast amounts of information. Failure of the stems can lead to false identification which can lead to unnecessary interrogations and procedures. The lack of control over who can see them is a clear infringement of privacy, and it is facial recognition technology's most apparent, obvious flaw. When a person is scanned by a camera, his or her anonymity is lost. FRT basically invades everyone's privacy to find one specific person. (Reynolds, 2015)

3.2 Fairness

If FRT is to follow the ethical principle of fairness, judgments must be made in such a way that everyone is treated equally. FRT, on the other hand, deviates from a fairness approach due to scanning of all people.

With facial recognition camera serving as society's watchful eyes, a law-abiding citizen is evaluated in the same light as a criminal suspect. While it is fair that ill-intentioned individuals who have been discovered be prosecuted with legal matters, it should not be acceptable for the other citizens to be wrongly accused and constantly monitored.

3.3 Security

FRT can assist in improving the safety of both public and private areas. FRT systems can be used in highly populated areas, such as the stadium or fair, to scan the faces of all attendees. If a scanned image matches one in the database that designates a person as dangerous or sought, he or she can be closely tracked and monitored. This ability to detect a dangerous individual before he or she encounters a big group of people, without the deployment of extensive security detail or intrusive measures, helps to ensure the safety of many individuals. (Carzo, 2010)

4. Legal implications

4.1 Discrimination

Facial recognition technology is not 100 percent accurate. This accuracy may be as low as 65 percent in the case of women, children, and ethnic minorities. This means that, by its very nature, technology is discriminatory due to its less-than-ideal outcomes.

While this may change in the future as artificial intelligence technology scans and "discovers" a wider range of faces, it currently runs the danger of violating racial discrimination laws.

4.2 Privacy

The Commercial Face Recognition Privacy Act, introduced in the US Senate in March 2019, is one of the most current measures to tackle facial recognition. The Act aims to make legal changes that compel corporations to notify customers before acquiring face recognition data.

This is in response to the Biometric Information Privacy Act of Illinois (BIPA). Though not directly aimed at facial recognition, the act mandates that entities gain consent to collect biometric data, and that consent must be supplied voluntarily rather than by default.

Even today, companies that use facial recognition technology, such as Facebook and the Russian social media site VK, as well as government agencies, must be cognizant of the rules governing personal privacy in their jurisdictions and the safeguards that must be implemented.

4.3 Democratic freedom

The role of facial recognition technology and democratic freedom will be the final legal topic we will explore. The ideals of democratic freedom include the freedom to choose, as well as the freedom to gather and exchange information. Despite the various applications of facial recognition technology, this is one area where it fails.

These technologies capture and store large volumes of data, which is commonly done in the cloud. This raises the question of data security, as well as the danger of governments spying on its populations. It is a problem that will necessitate new legislation in addition to present democratic freedom laws. (Kuflinski, 2019)

4.4 Legal rules

There are currently no FRT-specific pieces of legislation in the EU or the UK, although there are other pieces of legislation that govern FRT management and implementation. In terms of personal data management, the EU's GDPR is often regarded as setting the bar at the highest level for personal data management.

The GDPR mandates the implementation of systems that include 'privacy by design' (PbD) and 'privacy by default' for any personal data processing. Personal data processing must have a clear legal basis, and the data must also be processed fairly and transparently. It's vital to note that this does not preclude the collecting of personal data; rather, it necessitates clearly documented methods and ongoing personal data management. Furthermore, it should be recognized that what is considered fair and legal is subject to interpretation, legal dispute, and contestation. Consent for processing is required in some cases. There are also specific data subject rights, such as the right to know what information is held on/about you, subject to certain exceptions, and the right to request that data be corrected or deleted in certain instances.

An example case shows how a data protection authority's independence and legal knowledge can ensure accountability in situations where an individual or a civil organization would not be able to do so for a variety of reasons. In this case, the IMY "found out through media reports" that the school was experimenting with FRT on its children and decided to interfere. Following this, the authority determined that the school's use of face recognition did not meet the requirements of proportionality and necessity, resulting in the DPIA being conducted wrongly. Most crucially, the IMY found that the children's parents' assent to the school was illegal because the students were in a dependent condition (school attendance is compulsory). The school’s board was subsequently fined approximately €20,000. (Almeida, et al., 2021)

5. Security for their users.

The proposed system is a final year project for my undergraduate study, so the project wont probably go live. But there exists a probability, so, written consent of collecting and processing data may have to be implemented in future. But as of now, the collection and processing of data will be implemented by introducing terms and conditions to users during initial signup/registration process.

Collection: Consent will be obtained from attendees as terms and conditions before including their data in the facial recognition database.

Fairness in Usage: The system will refrain from using facial recognition to determine an individual's skin color, race, religion, national origin, gender, age, or disability.

Disclosure: The data of a facial recognition system won't be traded or used without the informed consent of the involved person.

Access: Attendees should have the right to access, edit, and delete their facial information, along with records of any changes made to the data.

Misuse: The system will take proactive measures and appropriate controls to prevent their misuse. Some measures include restricting automated access to sensitive database related to an individual's identity.

Reliability and Security: The system will have dedicated security measures to host, manage, and secure facial recognition information.

Accountability: End-users will be able to keep an audit trail that includes information collection, use, and disclosure details, as well as date and time stamps and information on the users who requested the data.

Government access: System may grant the government access to confidential information under the Data Protection Act 1974 or upon receipt of a probable cause warrant.

Transparency: Organizations must create policies for data compliance and use, as well as the technical mechanisms required to ensure responsibility. (Gangarapu, 2022)

6. Conclusion

Ethics aside, not only FRT can provide a safer environment to live in, but also provide convenience and easier access to several everyday tasks. The ability to provide a less intrusive and/or obstructive method of security, while also increasing the safety of an extensive number of people, is clearly a benefit of FRT.

The argument can be made that FRT is ethical in some way, The ethical approach applies in this regard as a utilitarian approach. A utilitarian approach is one in which the intended technology created the best overall consequences for all people who might be affected, either directly or indirectly. Clearly, FRT can follow a utilitarian approach and benefit large amount of people in countless ways. (Carzo, 2010)

References

Almeida, D., Shmarko, K. & Lomas, E., 2021. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics.*

Andrejevic, M. & Selwyn, N., 2020. Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology,* 45(2), pp. 115-128.

Carzo, R., 2010. Under the W Under the Watchful E atchful Eye: The Highly Intrusiv e: The Highly Intrusive Natur e Nature of Facial. *The Review: A Journal of Undergraduate Research,* Volume 12, pp. 1-5.

Gangarapu, K. R., 2022. *Ethics of Facial Recognition: Key Issues and Solutions.* [Online] Available at: https://learn.g2.com/ethics-of-facial-recognition [Accessed 20 February 2022].

Joshi, N., 2021. *Ethics and Errors of Facial Recognition Technology.* [Online] Available at: https://www.allerin.com/blog/ethics-and-errors-of-facial-recognition-technology [Accessed 10 2 2022].

Kuflinski, Y., 2019. *How Ethical is Facial Recognition Technology?.* [Online] Available at: https://towardsdatascience.com/how-ethical-is-facial-recognition-technology-8104db2cb81b
[Accessed 18 February 2022].

Reynolds, G. W., 2015. *Ethics in information technology.* 5th ed. Bsoton: Cengage Learning.