Declaration on Plagiarism

Assignment Submission Form

This form must be filled in and completed by the student(s) submitting an assignment

Name(s):	Vinit Saini
Programme:	MSc in Computing - Blockchain
Module Code:	CA640I
Assignment Title:	Ethical issues in using facial recognition technology with a case study of Amazon's Rekognition: An AI & ML-based image and video analysis service
Submission Date:	16 November 2022
Module Coordinator: Renaat Verbruggen	

I/We declare that this material, which I/We now submit for assessment, is entirely my/our own work and has not been taken from the work of others, save and to the extent that such work has been cited and acknowledged within the text of my/our work. I/We understand that plagiarism, collusion, and copying are grave and serious offences in the university and accept the penalties that would be imposed should I engage in plagiarism, collusion or copying. I/We have read and understood the Assignment Regulations. I/We have identified and included the source of all facts, ideas, opinions, and viewpoints of others in the assignment references. Direct quotations from books, journal articles, internet sources, module text, or any other source whatsoever are acknowledged and the source cited are identified in the assignment references. This assignment, or any part of it, has not been previously submitted by me/us or any other person for assessment on this or any other course of study.

I/We have read and understood the referencing guidelines found at http://www.dcu.ie/info/regulations/plagiarism.shtml , https://www4.dcu.ie/students/az/plagiarism and/or recommended in the assignment guidelines.

Name(s): _____Vinit Saini_____ Date: ___16 November 2022_____

Ethical issues in using facial recognition technology with a case study of Amazon's Rekognition: An AI & ML-based image and video analysis service

1 Introduction

As a field of artificial intelligence (AI), computer vision is the ability of computers to analyse digital images, videos, and other visual inputs and take action or recommend actions based on that information. Computer systems use machine learning and artificial intelligence to learn and capture information from various sources of digital nature. The amount of digital data that is being generated daily is the main driving factor behind computer vision technology. This data is used to train the systems to understand the visual images better. The rapid growth of technology and the immense size of digital content produced in recent years have made it possible to derive useful information from such raw digital data. Computer vision enables machines to learn visual data and derive useful information to take appropriate decisions. Facial recognition is a specific field of computer vision. In general, it consists of techniques focused on discovering, examining, and interpreting the images to identify human faces.

According to Amazon, Rekognition is a service that runs on deep learning technology and can be used to identify objects, scenes, and faces. It can extract text, recognise celebrities and identifies inappropriate content in a given image. It supports face searching and comparison too. Rekognition service is based on Amazon's established, highly scalable infrastructure to work on billions of images having different sizes or qualities. To help one make informed decisions about how to use the results, Service also returns a confidence score for everything it identifies. (Amazon Web Services Inc., 2022)

As per the federal government accountability office report, approx. 42 federal agencies are known to use facial recognition technology in one form or another (Rainie *et* al., 2022). Similarly, Ring, the innovative doorbell company owned by Amazon, accounts for partnerships with more than 1,000 police agencies across the United States, per the tracker on Ring's official website (Ring, 2022). Such facial recognition software is intelligent software and surely helps in various real-world scenarios like enforcing the law, rescuing human trafficking victims, reuniting missing children with their families and many others. However, civil rights advocates have also raised concerns about potential racial bias in such surveillance technology. Such software could cause racial discrimination. In the past, Researchers have raised concerns about the potential possibility of producing inaccurate results, especially for people with darker skin. As per Allyn (2020), Some studies have shown that women and younger people can also be negatively impacted by technology. In one of the tragic incidents where a man named George Floyd was killed in police custody, followed by Amazon banning the police from using its facial recognition software. Amazon's Rekognition is part of the Amazon Web Services suite. The software uses machine learning to look for a match among hundreds of thousands of police records in a database containing images from social media accounts or smartphones of investigating officers. Critics have highlighted the possibility of wrong identification while using algorithms solely to identify people, this poses the risk of mistaken identity. Again, these technologies pose some serious concerns around ethics, like lack of transparency and consent in using facial data, mass surveillance, biased, and accuracy concerns are a few of the major ones.

2 Literature Review

2.1 Computer Vision and facial recognition

Computer vision is a specialised branch of artificial intelligence (AI). Computer vision includes techniques that allow task automation from a raw image or video clip. Facial identification or image recognition is not the only application of computer vision. Computer vision also covers applications like Iris recognition, Optical character recognition (OCR), Text recognition etc., which can be used to convert printed or handwritten content into digital files.

In comparison, facial recognition is a field of computer vision. It comprises the discovery, examination, and interpretation of facial data to aid the decision-making process. It operates on a neural network trained through several annotated datasets having raw data (Ewan, 2017). Face recognition serves the same purpose as computer vision, i.e., automating tasks. Facial recognition consists of various tasks such as labelling faces by way of tagging, understanding facial expressions for fear, fun, and happiness, or searching for a particular face through facial features among large datasets. It includes data classification, detection, segmentation or tagging. Facial recognition automatically recognises a face within a given raw image to determine the person's identity. The real-world applications can be seen in automated vigilance, biometrics verifications and robotics. Likewise, iris recognition is another form of biometric verification that can identify someone through their iris. Iris, the coloured portion of the eye, is composed of complex, unique patterns that can be used to identify people individually.

2.2 Usage of AI and ML in facial recognition software

Artificial intelligence and machine learning are the primary technologies behind face recognition. The AI algorithms search for standard facial features like human eyes, eyebrows, nose, mouth, nostrils and iris. Once this data is fed into the system, additional validations using large datasets which contain both positive and negative images can be used to confirm the human face. Few standard facial recognition techniques are based on features, appearances, knowledge, and template-matching, which provides various methods to achieve these goals. Each has its benefits and shortcomings.

Feature-based methods rely on facial attributes such as eyes or nose to detect a face. Hence, noise and light interference could cause variations in outcomes. Further, methods based on appearances use statistical analysis and some machine learning algorithms to match the image of a face. This approach uses predefined rules to recognise a face. Such an approach needs a considerable amount in terms of effort and time to define well-defined rules.

In contrast, template-matching methods are based on comparing facial images with existing data stored in databases and correlating the results to identify a face in an image. Although, this method must consider scale, pose, and shape variations (Suneratech, 2021).

Artificial Intelligence and machine learning aim to provide great opportunities and countless possibilities to improve our surroundings. However, consideration of ethics and the privacy of people is paramount while dealing with personally identifiable data (PII).

2.3 AI-related Challenges

There are three broad types of challenges: Technology-related, Privacy-related, and Ethical. Ethical and privacy concerns are the main challenges that cause these technologies not to be widely adopted in modern computer vision software. In contrast, the technological challenges seem to dissolve away with the rapid innovation progress in the industry. Most AI systems need training before they can be used. It requires the use of a training data set, which in the context of images and videos of general

nature, might involve personal information of people in those images which facilitates the algorithm to recognise faces and people. Data privacy and data consent are challenging in such cases.

2.4 Ethical Challenges

The use of artificial intelligence uncovers difficult questions and some ethical dilemmas. Ethical challenges greatly limit the advocacy of the use of this technology in enforcing the law and surveillance. Prominent dilemmas and concerns among all are, how AI ensures fairness? how people's privacy will be maintained? and what's the level of contextual integrity? Or Are AI technologies dangerous if there is high dependence on them?

Narayanan (2018) defines that there are around 21 definitions of fairness in computer science. For example, fairness can be seen as means of equal opportunity. Alternatively, fairness can also be seen as free from any type of bias commonly based on gender, colour or race. Nevertheless, another definition could be seen as an equal standard while judging people across interpersonal and legal dimensions. In sum, even though it is vague, it remains an essential moral value people expect from AI systems. Nevertheless, it can be considered one of the most seen ethical issues in software.

Fairness is tricky to optimize since it encompasses several different aspects, some of which are mutually exclusive. For example, a law enforcement agency should provide equal enablement of law and order without any bias. Historically or intrinsically disadvantageous groups will not be considered fair by the technology, therefore, implementing an AI-based system that considers such dilemmas is not straightforward, and might often need to account for some sacrifices.

Since law enforcement agencies capture the data for social betterment, they can use it as they deem fit. Although, such an assumption again can pose other ethical issues regarding data ownership. As AI systems become faster and more accurate in mimicking human decisions, a law enforcement agency might depend more on AI than human judgements. Considering this fact, Would law enforcement agencies eventually be unable to make decisions without AI assistance?

A major ethical issue of facial recognition is that such technologies often use personally identifiable information without explicit consent or notification to the owner of the information.
Accessing surveillance cameras, images, and video footage of employees, customers, or the general public should only be allowed when all of the affected parties are well aware of the usage of their personal information. Facial recognition of someone further opens the potential to access other forms of personal information, which can further exaggerate ethical concerns. For instance, what if a storekeeper uses facial recognition software to identify customers with sound purchase history or financial background? Is it wise to avoid serving customers with not-so-good purchase histories and focus instead on lucrative customers? Wouldn't it be a biased treatment? How about fetching personal details on the basis of facial recognition?

3 Liffick's analysis

The following section uses Liffick's analysis methodology of Amazon's facial recognition software.

3.1 Participants and their Actions

<u>Primary participants</u>

- The company (Amazon Inc.): the company that developed and provided the AI-based face recognition tool to law enforcement agencies to help solve the cases.
- Federal law enforcement agencies: people using face recognition technology to assist law enforcement and solving cases.

- Civil rights groups and police-reform advocates: advocates of human rights. It also involves people who demand reforms in police ways of doing and software-assisted decision-making.
- Federal government: responsible for guardrails using facial recognition technology.

Secondary participants

- Reporter (CNBC): published a report on 10 June 2020 about Amazon banning police to use facial recognition technology for one year, yielding pressure from police-reform advocates and civil rights groups.
- Victims: people wrongly picked up by the software and hence victims of mistaken identity.
- Civil rights groups and police-reform advocates: who analysed the system's shortcomings in respect of mistaken identity and identified the need for reforms.

Implied participants

- Researchers: people behind the technology who argues the benefits and shortcoming of such software.
- Technology critics: advocate the need to deploy stronger regulations of facial recognition technology to govern ethical usage of technology.
- Developers: built the AI tool that automatically compares and recognises people from federal databases for potential criminals.

3.2 Reduced List

- The company (Amazon Inc.): As responsible for developing the tool.
- Developers: As responsible for developing the algorithms that could produce biased results, causing mistaken identity errors.
- Law enforcement agencies: As primary users of the system, uses the results of the system for decision-making.

3.3 Legal Considerations

- Race, Ethnicity, or National Origin-Based Discrimination Act. - If the software is biased or produces incorrect results for a particular set of people, it violates this law, providing equal recognition rights despite their colour, race, ethnicity, age or sex (ACLU, 2022). Many studies in the past have shown the biased nature of results produced by facial recognition technology, especially technology is prone to produce incorrect results for people with darker skin, women and younger people.
- General Data Protection Regulation: A couple of significant points that GDPR states such as a company must take implicit consent from the data owner to process their data, including photographs used to train the visual recognition models. Also, companies must be transparent in their data policies in respect of data usage and keeping it with them. (GDPR, 2022)

3.4 Possible Options for Participants

- Company
  - They could have researched the implications and possible challenges of using AI-based facial recognition systems.
  - They could have relied on extensive training for their models on diversified data sets to reduce the chances of error or biased results.
- Developers

    - They could have done a statistical analysis of the training data set. Such analysis techniques usually reveal the possibilities of data skewness in advance.
    - Moral and ethical requirements should have been considered as implicit functional requirements.
- Law enforcement agencies
    - In place of such tools, human effort could have been used to accomplish the task.
    - Should have considered moral and ethical sense while making decisions.

3.5 Possible Justifications for Actions

- The Company
    - Possibly, this is a new technology and therefore needs time to mature regarding privacy, morality or ethics.
    - Again, in real-world use cases, boundaries are not fully defined and lack strict regulations around technology.
- Developers
    - Since the technology is relatively new thorough and diversified training data sets are required to train the models better.
    - Also, due to the lack of concrete regulations around technology usage, it is not prominent for developers to consider the questions of morality and ethics.
- Law enforcement agencies
    - As per the report, Law enforcement agencies found facial recognition software to be a handy tool for identifying and searching suspects across thousands of profiles in federal databases.
    - Ease of use helps in quick decision-making for the agencies.

3.6 Key Statements

- "Research has indicated that facial recognition software may hold racial and gender bias."
- "A Massachusetts Institute of Technology study demonstrated that while men with lighter skin were often almost always positively identified, about 7% of women with lighter skin were misidentified, and up to 35% of women with darker skin were falsely identified."
- "… it is banning the use of its facial recognition software by police for one year, as pressure on tech companies builds to respond to the killing of George Floyd by a police officer in Minneapolis."
- "...one-year moratorium might give Congress enough time to implement appropriate rules."
- "...calling for an outright national ban on facial recognition technology and says Amazon's one-year break appears strategic."
- "...advocated that governments should put in place stronger regulations to govern the ethical use of facial recognition technology."
- "...IBM said it was exiting the facial recognition business, … calling on Congress to enact reforms to advance racial justice and combat systemic racism."
- "The reality is that facial recognition technology is too dangerous to be used at all."

3.7 Questions raised

- Has the company considered the moral and ethical implications of this technology and software implementation?
- Did the developers analyse the data used for training the AI system?
- Was there proper testing of the solution across diversified data sets?

- Data owners' consent obtained for AI training?
- Was enough training given to the enforcement agencies to use the software results in decision-making based on ethics and morality?
- Were there any external influences in the decision-making process?

3.8 Analogies

- Dastin, J. (2018). "Amazon scraps secret AI recruiting tool that showed bias against women" Available at: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G
- Berlatsky, N. (2018). "Google search algorithms are not impartial. They can be biased, just like their designers" Available at: https://www.nbcnews.com/think/opinion/google-search-algorithms-are-not-impartial-they-are-biased-just-ncna849886

3.9 Codes of Ethics Comparison

- Ethics of personal data: Data owners' consent must be obtained in advance in respect of usage and time to keep. Using anonymous data is an excellent practice when the research does not require identity. Ensure sufficient confidentiality levels when making data available for reuse.
- Professional Ethics: Such ethical values help to define standards for acceptable behaviour by law enforcement agencies.
- Business ethics: Such ethical values help a company to define and maintain standards of acceptable behaviour in a business context.
- Ethics of anonymity: A set of ethics allows someone to remain anonymous online.

4 Alternative Proposals

- Pessimistic: Company should have evaluated other mature technologies to mimic complex human decision-making rather than AI technology which is not fully grown yet.
- Optimistic: Company could consider optimising their AI-based system to mimic human decisions to prevent any possible bias via design-level modifications. Again, ensure thorough testing of the system is done to achieve the expected level of correctness and to ensure the system is free from bias or other issues before deployment.
- Compromise: Company to test the system thoroughly and have a human representative who can verify the decisions provided by AI systems periodically. AI systems can do the heavy lifting of recognising and comparing the suspects. However, human officers would have the final say on the last decision.

5 Conclusion

The objective of the amalgamation of AI technologies into traditional law enforcement and detective work is to make the investigation process efficient and less human-labour intensive. However, decision-making through AI systems is a relatively new concept. Implications like data privacy, ethics, and the need for such a system in the investigation process are to be considered carefully by every legislation before implementation in the real world, once implemented there must be frequent checks to ensure that the AI system is behaving as expected and is within the acceptable operational boundaries. There is no doubt that AI could speed up the investigation process and save human efforts to a great extent. However, Misuse of technology in unethical ways could result in a loss of trust and faith in the investigation or law enforcement agencies reputation.

Bibliography

Amazon Web Services, Inc. (2022) *Amazon Rekognition Image*. Available at: https://aws.amazon.com/rekognition/image-features/ (Accessed: 16 November 2022).

Rainie, L., Funk, C., Anderson, M. and Tyson, A. (2022) *Public more likely to see facial recognition use by police as good, rather than bad for society.* Available at: https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/ (Accessed: 16 November 2022).

Ring (2022) *Active Agency Map*. Available at: https://support.ring.com/hc/en-us/articles/360035402811-Active-Agency-Map (Accessed: 16 November 2022).

Allyn, B. (2020) *Amazon Halts Police Use Of Its Facial Recognition Technology* Available at: https://www.npr.org/2020/06/10/874418013/amazon-halts-police-use-of-its-facial-recognition-technology (Accessed: 16 November 2022).

Ewan (2017) *Difference between computer vision and image recognition* Available at: https://deepomatic.com/difference-between-computer-vision-and-image-recognition (Accessed: 16 November 2022).

Suneratech (2021) *What Is AI, ML & How They Are Applied to Facial Recognition Technology* Available at: https://www.suneratech.com/blog/ai-ml-and-how-they-are-applied-to-facial-recognition-technology/ (Accessed: 16 November 2022).

Narayanan, A. (2018) *21 fairness definitions and their politics* Available at: https://fatconference.org/static/tutorials/narayanan-21defs18.pdf, p. 1 (Accessed: 16 November 2022).

American Civil Liberties Union (2022) *Know tour rights: Race, Ethnicity, or National Origin-Based Discrimination* Available at: https://www.aclu.org/know-your-rights/discrimination-on-the-basis-of-race-ethnicity-or-national-origin (Accessed: 16 November 2022).

General Data Protection Regulation (GDPR) (2022). *Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR).* Available at: https://gdpr-info.eu/art-5-gdpr/ (Accessed: 16 November 2022).

Gangarapu, K. R. (2022) *Ethics of Facial Recognition: Key Issues and Solutions* Available at: https://learn.g2.com/ethics-of-facial-recognition (Accessed: 16 November 2022).