Facial Recognition

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions? Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

Mollie and Daisy are first time mothers and the victims of bullying by their neighbors. They have been hurt to such an extent that they have stopped eating and are not capable of working or feeding their children. They can't even tell others who the bullies are. The landlords where Mollie and Daisy live recently began using facial recognition technology to identify the bullies. Mollie and Daisy are two of thousands of cows living on a dairy farm that had been losing huge profits due to decreasing milk production due to injured cows. Thanks to the new technology, the farmers have been able to regain their profits and keep the cows safe. In a different context, but with a similar motive, Taylor Swift used facial recognition technology in her 2018 California concert to identify and isolate potential stalkers.

Facial recognition systems work by using artificial neural networks. This doesn't involve a computer programmer writing codes about hair and skin color or specific facial features. Instead, the neural network is trained using algorithms to recognize patterns and traits by analyzing data beginning at the pixel level. The process is guided by humans, who feed data to the neural network and make adjustments when the network makes mistakes. But in the end, the network, not the creator, makes decisions about which similarities and differences are significant in facial recognition. Advances in cloud computing, machine learning and digital cameras have all contributed to developments in facial recognition. However, the Internet has made the greatest contribution of all. One database is said to hold over ten million images gathered from social media networks, dating and photo websites and from security cameras placed in public places. Unlike fingerprints or iris scans, faces are recorded without knowledge, let alone consent, of the people to whom they belong. Recently, Microsoft and Stanford University in the US have announced that they are removing face databases from the Internet, but due to the widespread distribution of these images, chances are your face is already on another database.

Facial recognition technology has the potential to assist police in identifying criminals, as well as locating missing people. Facial recognition can be useful in the diagnosis of illnesses even before the person realizes they are suffering. Blood pressure and pain levels can be monitored without the presence of a medical doctor.

Despite potential benefits, a number of concerns have been expressed about the use of facial recognition. A MIT study titled Gender Shades has reported that IBM and Microsoft provide more accurate recognition of white men's faces than any other faces. An error of up to 35% has been recorded in the identification of non-whites, women and children. While we may believe that machines are neutral, facial recognition algorithms repeat the conscious and unconscious biases of the people who created and trained them.

Some have argued for a need for government oversight in the use of facial recognition as a way to curb potential abuse. The London Metropolitan Police retains thousands of images of people who were found to be innocent of the crimes of which they were accused. Yet, these innocent faces will continue to be used for future police searches. In May 2019, San Francisco became the first American city to ban the use of facial recognition software by police. This was in response to inaccuracies in facial recognition as well as concerns that facial recognition violated privacy laws. Others are concerned that government oversight can quickly lead to constant surveillance of citizens. The Chinese government, over the period of only one month, scanned 500,000 faces of a racial minority called the Uighur; the Uighur are also China's largest Muslim population and a racial minority in the country. A national digital panopticon system has been created and some are worried that it could be used to identify hundreds of thousands of Uighurs and place them in concentration camps.

The UAE has been at the forefront of adopting facial recognition technology to be used for a variety of purposes, primarily for security. Starting in 2018, the Dubai police started installing the technology into thousands of existing street cameras. The police department says that the ultimate goal is a future without policemen and where the crime rate is zero. Some Muslim residents, however, feel that not only is this a violation of privacy, but also culturally and religiously inappropriate and unacceptable. Moreover, a Dubai-based firm, NNTC, has been involved in the production of facial recognition-enabled smart glasses that will be deployed by law enforcement and security anytime, anywhere, in the UAE. And self-driving vehicles, which are expected to be on the roads by EXPO 2020, will make facial recognition ubiquitous, scanning not just the surrounding environment of the car, but every face of every person passing by.

Word count: 795
FK 12

References

Conger, K. Fausset, R. and S. F. Kovaleski. (2019, May 14). San Francisco bans facial recognition technology. *The New York Times*. Retrieved from https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Dennehy, J. (2018, April 10). Street cameras that scan every face and hear every conversation could be coming to UAE. *The National*. Retrieved from https://www.thenational.ae/uae/street-cameras-that-scan-every-face-and-hear-every-conversation-could-soon-be-coming-to-uae-1.720390

Kuflinski, Y. (2019, April 11). How ethical is facial recognition technology? *Towards Data Science*. Retrieved from https://towardsdatascience.com/how-ethical-is-facial-recognition-technology-8104db2cb81b

Metz, C. (2019, July 13). Facial Recognition Tech Is Growing Stronger, Thanks to Your Face. *The New York Times*. Retrieved from https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html

Mozur, P. (2019, April 14). One month, 500,000 face scans: How China is using AI to profile a minority. The New York Times. Retrieved from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Owen, D. (2018, December 17). Should we be worried about computerized facial recognition? *The New Yorker.* Retrieved from https://www.newyorker.com/magazine/2018/12/17/should-we-be-worried-about-computerized-facial-recognition

Vincent, J. (2019, June 10). Facial recognition smart glasses could make public surveillance discreet and ubiquitous. *The Verge*. Retrieved from https://www.theverge.com/2019/6/10/18659660/facial-recognition-smart-glasses-sunglasses-surveillance-vuzix-nntc-uae