Facial recognition: How South Wales Police caught a sexual predator

https://www.bbc.com/news/uk-wales-55842869

Group FR 3
Matthew Morgan, Sihan Xu, Mike Adams, Andrew Geyko

One of the concerns our group came up with was the ethics behind targeting only criminals in facial recognition searches. We believe that this kind of stance towards the issue does not take into account people reforming and also may unfairly target those who have committed petty crimes in their youth. There is also concern about whether or not a system such as this will target groups who are disproportionately arrested. Our solution to this issue is to use this system more selectively, such as only having wanted or violent offenders showing up in the facial recognition database or using the system only when “high-profile” crimes are committed (the exact definition of this can of course be debated endlessly). A balancing act between citizen privacy and citizen safety is a very fragile wire to walk on and any technology or law that affects one or the other should be treated critically and skeptically.

Another criticism of the article is that it does go into specifics about the facial recognition technology that was used. It only stated that comparison of faces used were of people with past criminal convictions. Explaining more about the database used for comparisons, the name of the technology and who created it, or the process of determining the correctness of a match are some examples of items that could go along with what was in the article.

Using facial recognition software on situations that only demonstrate intent of the crime may be a human rights concern. The databases used within facial recognition software packages should be closely monitored, if possible, to try and remove bias. Choosing the organization that decides on the structure of the database would be an ethical dilemma, as well. In a related situation, it would be better to restrict access to facial recognition to certain groups within law enforcement, so that people do not attempt to abuse it consistently.

From the technical, the face is the only biometric information that can be collected without the user's active cooperation. The collection process of other biological characteristics, such as fingerprints, palm prints, iris, veins, and retina, requires the active cooperation of the user as the premise, that is, if the user refuses to collect, high-quality characteristic information cannot be obtained. From the social psychology, identifying identity through face conforms to the human visual recognition experience and is easily accepted by users. For example, when people collect fingerprints and iris, they worry about privacy leakage, but they are photographed by hundreds of surveillance cameras on the street every day, but they don't feel infringed, because the face

is naturally exposed and is considered a natural feature for identification. Due to the above two points, the risks of face recognition technology are easily overlooked. Unlike biometrics such as fingerprints and iris, faces are generally not used to identify specific identities, but to identify suspects. At entry and exit ports, airports, stations, casinos, and other places, face recognition technology can compare the user's face image with the face image of the suspect list without the user's knowledge. With the help of surveillance cameras densely distributed on the streets, face recognition technology can squat, stalk, and track targets 24 hours a day, tirelessly and sleeplessly. Obviously, the list of suspects can be replaced with any list, such as being used for illegitimate purposes other than maintaining public safety, without any technical difficulty. In a centralized country, face recognition technology can become Big Brother's most powerful surveillance tool, just like the "Eye of Sauron" in The Lord of the Rings. Regardless of the end of the world, day and night, I will always watch you without blinking for a moment.