The reference information for the article :

Title: How Facial Recognition Technology Could Help Catch Criminals,

Author: Cadie Thompson,

Published: 19 April 2013,

Link: https://www.cnbc.com/id/100656156

A summary of the content of the article:

The article is mainly about law enforcement using facial recognition technology to catch suspects or criminals. This technology was seen to the public by being used in identifying the two Boston bombing suspects. The facial recognition software uses digital images of suspects to match their identities within a few minutes. The database they searched belongs to government agencies. However, the firm that provides the facial recognition technology said they may also access some foreign firms whose database was speculated to contain the suspect's data. Additionally, facial recognition technology requires the image with high quality to reach the high accuracy to match the person within the database. The low-quality image often released by enforcement may not be effective in finding the solution. The baseline is 90 pixels of resolution between the two eyes of the pictured person. So they often use software to create an image of the suspect. This additional layer of software turns the match into a probability game. The law enforcement would get several potential matches of the suspect at last.

The ethical question of facial recognition technology is the choice between public good and expendable privacy. This use of facial recognition technology probably accesses a good amount of quality data of citizens, and the software that creates the image of the suspect could cause errors. This technology may have crossed privacy boundaries. The trampled the privacy of the citizens may seem expendable. The guessing game between potential suspects that were selected by a created image is totally some arbitrary choice and guesswork. But law enforcement may argue it is for the greater good that at least it is helpful to identify a lot of suspects. In the law enforcement context, facial recognition technology is a fairly benign tool that is designed to prioritize specific interests in police matters. Additionally, we must consider its longer-term implications, it is not just harmful and unethical to public privacy now, but in the future, the government may use such technology to track down dissidents and crime syndicates and foreign espionage organizations may identify citizens or public servants if the technology is leaking.

The ethical issue may reach a pragmatic solution by enhancing the supervision of the use of facial recognition technology and access to the database. The people or organizations who access the data of citizens must be strictly on the whitelist. While the use increases the flow of the data, it also expands the potential of hackers to loot the data, so the evolution of facial recognition technology security and data encryption is also on schedule. The government may hire some ethical hackers to do penetration tests to find vulnerabilities in the system. The authorized hackers must obey the specific guidelines to perform hacking for law enforcement legally. Law enforcement must keep an eye on insider information because they know the intricate details of the architecture and how to exploit it. The government also must turn an active defense against foreign hacker organizations because the database and the facial recognition technology may be the prioritized specific interests of the foreign government. If the defense task is too expensive, they may also consider the physical isolation of facial recognition technology and access to the database. Physical isolation may limit the use of the technology but it is practical for law enforcement who lack funds. In conclusion, law enforcement must find the delicate balance point between security, privacy, and efficiency.