GUIDING PRINCIPLES FOR LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

What is Facial Recognition:

Facial recognition technology automates the process of comparing one photograph to other photographs to find potential matches. Facial recognition is a software application capable of potentially identifying or verifying the identity of a person by analyzing patterns based on a person's facial feature locations and contours and comparing them to those features in other photographs. The primary government applications for facial recognition in the United States are identity verification, security, and law enforcement investigations.

What Facial Recognition is NOT:

The result of facial recognition analysis is NOT a positive identification of an individual. In the law enforcement investigations context, facial recognition is a tool that potentially develops an investigative lead. Once the potential lead has been generated, human intervention is required to determine if the person in a photograph is actually the person whose identity is in question.

Principle One:

It is the responsibility of the user agency to develop appropriate facial recognition technology usage policies in accordance with the applicable laws and policies of the governmental jurisdiction to which the user agency is subject. In response to the expanding use of new and emerging technologies, the International Association of Chief's of Police (IACP) released a Technology Policy Framework to guide the development and support policies that ensure responsible and effective deployment and use of technologies.

Principle Two:

All appropriate use policies must protect the constitutional rights of all persons and should expressly prohibit any use of the technology that would violate an individual's rights under the First and Fourth Amendments.

Principle Three:

The results returned in a facial recognition candidate list are ranked based on computational analysis of the similarity of features. The candidate list may include photos of individuals who may be of a different race, gender, and/or age than the individual in the submitted probe photo.

Principle Four:

The images and information contained in the candidate list are for investigative lead generation purposes only, and are not to be considered as positive identification, or used alone as the basis for any law enforcement action.

Principle Five:

Before access to any facial recognition system is authorized, a law enforcement agency should require individual users to participate in training on how the facial recognition system functions, its limitations, the importance of using high resolution equipment and images, and the interpretation of results, as well as the implementation of and adherence to the agency's facial recognition policy.

To access the IACP Technology Policy Framework, please click on the IACP web link::
https://www.theiacp.org/iacp-technology-center

To access the IACP/IJIS Facial Recognition Use Case Catalog, please click on the IJIS Institute web link:
https://www.ijis.org/news/news.asp?id=439103&terms=%22facial+and+recognition%22

Law Enforcement Imaging Technology Task Force (LEITTF)

A joint effort of the IJIS Institute and the International Association of Chiefs of Police

July 2019