NORTHAMPTON POLICE DEPARTMENT **Administration & Operations Manual**	
Policy: Facial Recognition Technology	**AOM: O-409**
Massachusetts Police Accreditation Standards Referenced:	Issuing Authority Jody Kasper Chief of Police
Dissemination Date: 07/01/21 **Effective Date:** 07/01/21	**Amended:** **Reviewed:** 10/23

Table of Contents

I. Introductory Discussion

It is the purpose of this policy to provide Northampton Police personnel with guidelines regarding the use of Facial Recognition Technology. The use of this technology is highly controversial and therefore, its use by police personnel is restricted both in Massachusetts and in the City of Northampton.

II. Definitions

Facial Recognition Technology (FRT): Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves or deceased persons.

III. The 2020 Massachusetts Reform Law

A. In December, 2020, the Governor signed into law, “An Act Relative to Justice, Equity, and Accountability in Law Enforcement in the Commonwealth.” The law includes a section specific to the use of facial recognition technology. The law indicates:

Any law enforcement agency performing or requesting a facial recognition search using facial recognition technology shall only do so through a written request submitted to the Registrar of Motor Vehicles, the Department of State Police or the Federal Bureau of Investigation.

A law enforcement agency may perform such a facial recognition search for the following purposes:

1. *To execute an order, issued by a court or justice authorized to issue warrants in criminal cases, based upon specific and articulable facts and reasonable inferences therefrom that provide reasonable grounds to believe that the information sought would be relevant and material to an ongoing criminal investigation or to mitigate a substantial risk of harm to any individual or group of people; or*

2. *Without an order to identify a deceased person or if the law enforcement agency reasonably believes that an emergency involving substantial risk of harm to any individual or group of people requires the performance of a facial recognition search without delay. Any emergency request shall be narrowly tailored to address the emergency and shall document the factual basis for believing that an emergency requires the performance of a facial recognition search without delay.*

Nevertheless, a law enforcement agency may:

1. *Acquire and possess personal electronic devices, such as a cell phone or tablet that utilizes facial recognition technology for the sole purpose of user authentication.*
2. *Acquire, possess, and use automated video or image redaction software; provided, that such software does not have the capability of performing facial recognition or other remote biometric recognition; and,*
3. *Receive evidence related to the investigation of a crime derived from a biometric surveillance system; provided that the use of a biometric surveillance system was not knowingly solicited by or obtained with the assistance of a public agency or any public official in violation of the law.*

Law enforcement agencies shall document each facial recognition search performed and shall provide such documentation quarterly to EOPSS. Such documentation shall include:

a) *A copy of any written request made for a facial recognition search.*
b) *The date and time of the request.*
c) *The number of matches returned, if any;*
d) *The database searched.*
e) *The name and position of the requesting individual and employing law enforcement agency.*
f) *The reason for the request, including, but not limited to, any underlying suspected crime.*
g) *The entity to which the request was submitted; and*
h) *Data detailing the individual characteristics included in the facial recognition request. Such documentation shall not be a public record, except for as provided for in (d).*

IV. City of Northampton Ordinance Prohibiting the Use of Facial Recognition Technology

A. On December 19, 2019, the City Council in the City of Northampton passed an ordinance limiting the use of FRT by City employees. City ordinance Chapter 290, section 1is titled, *Use of Facial Recognition Systems by Municipal Agencies, Officers, and Employees*.

B. The ordinance includes the following definitions:

1. “Face surveillance” refers to an automated or semi-automated process that assists in identifying an individual by capturing information about an individual based on the physical characteristics of an individual’s face.
2. “Face surveillance system” is any computer software or application or other technology that performs face surveillance.
3. "City official" shall include all officials and employees of the City, whether elected or appointed.

C. The ordinance states, “It shall be unlawful for any city official to expend any city resources to obtain, retain, access, or use any face surveillance system.”

D. Although the MA general law allows FRT to be used in certain conditions, the local Northampton ordinance prohibits the use of this technology. Therefore, all NPD officers must comply with the local ordinance and may not use this technology in any investigation.