PLANNING AND DEPLOYMENT

TRANSMITTAL OF WRITTEN DIRECTIVE

FOR SIGNATURE OF: James E. Craig, Chief of Police

TYPE OF DIRECTIVE: Manual Directive 307.5

SUBJECT: FACIAL RECOGNITION

ORIGINATED OR REQUESTED BY: Planning, Research and Deployment

APPROVALS OR COMMENTS:
The above referenced directive is updated to reflect the Board of Police Commissioners and internal review.

AFTER THE DIRECTIVE IS APPROVED AND SIGNED, PLEASE RETURN TO PLANNING AND DEPLOYMENT.
1301 Third Street, 7th Floor, Detroit MI 48226

Series	Effective Date	Review Date	Directive Number
300 Support Services		Annually	307.5
Chapter 307 – Information System			
Reviewing Office Crime Intelligence			☒ New Directive ☐ Revised
References:			

FACIAL RECOGNITION

307.5 - 1 PURPOSE

The purpose of this policy is to establish acceptable use for the Detroit Police Department's (DPD) facial recognition software. Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active or ongoing Part 1 Violent Crime investigation or a Home Invasion I investigation. If a match is found through DPD's Facial Recognition Process, it shall be considered an investigative lead, and the requesting investigator shall continue to conduct a thorough and comprehensive investigation.

307.5 - 2 Definitions

307.5 - 2.1 Biometric Data

Data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and facial recognition data.

307.5 - 2.2 DataWorksPlus

The facial recognition software with which the Department has a contract.

307.5 - 2.3 Examiner

An individual who has received advanced training in the facial recognition system and its features. Examiners have at least a working knowledge of the limitations of facial recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for facial recognition searches and to perform one-to-many and one-to-one facial image comparisons.

307.5 - 2.4 Facial Recognition (FR)

The automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity. All Facial Recognition searches must be corroborated by at least two examiners and one supervisor.

307.5 - 2.5 Highly Restricted Personal Information
An individual's photograph or image, social security number, digitized signature, medical and disability information.

307.5 - 2.6 Home Invasion I
Unlawful entry of a dwelling with intent to commit or committing a felony, larceny, or assault on the home when either the unlawful entrant is armed with a dangerous weapon or when another person is lawfully present in the dwelling.

307.5 - 2.7 Part 1 Violent Crimes
For the purposes of this directive, Part 1 Violent Crimes are defined as robbery, sexual assault, aggravated assault, or homicide.

307.5 - 2.8 Personally Identifiable Information (PII)
Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

307.5 - 2.9 Reasonable Suspicion
The specific facts and reasonable inferences drawn from those facts to convince an ordinarily prudent person that criminality is at hand.

307.5 - 2.10 Statewide Network of Agency Photos (SNAP)
A computer application managed by the SNAP Unit, deployed through the Michigan Criminal Justice Information Network (MiCJIN) portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

307.5 - 3 Prohibited Uses

307.5 - 3.1 Surveillance
Members shall not use facial recognition to surveil the public through any camera or video device.

307.5 - 3.2 Live Streaming or Recorded Videos
Members shall not use facial recognition on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source.

307.5 - 3.3 Mobile Facial Recognition
Members shall not use mobile facial recognition.

307.5 - 3.4 Predictive Analysis
Members shall not use facial recognition for predictive analysis.

307.5 - 3.5 First Amendment Events

The Detroit Police Department will not violate First, Fourth, and Fourteenth Amendments and will not perform or request facial recognition searches about individuals or organizations based solely on the following:

a. Their religious, political, or social views or activities;
b. Their participation in a particular noncriminal organization or lawful event; or
c. Their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

307.5 - 3.6 Facial Recognition Use for Immigration Enforcement

DPD members are strictly prohibited from using facial recognition to assess immigration status.

307.5 - 4 Discipline

Any violations to this policy shall be deemed major misconduct. Any misuse of the facial recognition software will be investigated and reviewed for criminality. The remedy for this misconduct is dismissal from DPD.

If facial recognition is used contrary to section 307.5 -3.5 First Amendment Events, DPD shall notify the Board of Policy Commissioners, the Mayor of Detroit, City Council President, and City Council President Pro Tem within 24 hours of the violation.

307.5 - 5 Use of Facial Recognition Technology

307.5 - 5.1 Use Limited to Still Images

Facial recognition software may only be used on a still image of an individual.

307.5 - 5.2 Criminal Investigation Required

Members shall not use facial recognition technology unless that technology is in support of an active or ongoing Part 1 Violent Crime investigation (e.g. robbery, sexual assault, or homicide) or a Home Invasion 1 investigation.

307.5 - 5.3 Individualized Targeting

Members shall not use facial recognition technology on any person unless there is reasonable suspicion that such use of facial recognition technology will provide information relevant to an active or ongoing Part 1 Violent Crime investigation or a Home Invasion I investigation.

307.5 - 5.4 Process for Requesting Facial Recognition

1. Requests for facial recognition services shall be submitted to the Crime Intelligence Unit (CIU), with photograph(s) to be reviewed, the incident number, the crime type, and other pertinent information. Photographs shall be handled as specified in Manual Directive 306.1 Evidence Property.

2. CIU shall perform facial recognition searches utilizing the Statewide Network of Agency Photos (SNAP) which include criminal mug shot images. In the event additional analysis is needed for confirmation of an investigative lead, a formal request may be made to MSP to search the state's database. Any such request must be approved by a CIU supervisor.
3. If the examiner detects an investigative lead, the examiner must corroborate this lead with at least one other examiner and a CIU supervisor. The corroboration must have written sign-off by the supervisor and all examiners' involved.
4. Upon final approval, CIU shall complete a supplemental incident report for the requestor. The supplemental incident report shall detail how the examiner came to their conclusion, and include the following language:
    a. "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigation and investigative resources."
5. In the event that a viable candidate cannot be located, the requestor will be notified that no candidate was identified.
6. If CIU cannot discern a viable candidate, the photograph of the suspect will be removed from the facial recognition system.

307.5 - 5.5 Outside Agency Using Facial Recognition

An outside agency, or investigators from an outside agency, may request searches to assist with investigations only if the following requirements are met:

a. Prior to making the request, the outside agency has a formalized agreement (e.g. a memorandum of understanding or an interagency agreement) between the Detroit Police Department and the outside agency;
b. The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in this directive and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:
    - "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigation and investigative resources."
c. If any agency is found not in compliance with this Directive, the Department shall immediately suspend all Facial Recognition requests until the requesting agency becomes in compliance with this Directive.

307.5 - 6 Governance and Oversight

307.5 - 6.1 LASO & Crime Intel Responsibilities

1. The primary responsibility for the operation of the Department's criminal justice information systems, facial recognition program and system, operations, and the coordination of personnel, the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Local Agency Security Officer (LASO) who is assigned to Technical Services.

2. The LASO will be responsible for the following:

    a. Overseeing and administering the facial recognition program to ensure compliance with applicable laws, regulations, standards, and policy;
    b. Acting as the authorizing official for individual access to facial recognition information;
    c. Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status; and
    d. Ensuring that random evaluations of user compliance with system requirements along with this policy and applicable laws are conducted and documented;

3. The commanding officer of the Crime Intelligence Unit will be responsible for the following:

    a. Reviewing facial recognition search requests, reviewing the results of facial recognition searches, and returning the most likely candidates – or candidate images – if any, to the requestor.
    b. Ensuring that protocols are followed to ensure that facial recognition information (including probe images) is automatically purged in accordance with this Department's retention policy, unless determined to be of evidentiary value;
    c. Confirming, through random audits, that facial recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy; and
    d. Ensuring and documenting that personnel (including investigators from external agencies who request facial recognition searches) meet all prerequisites stated in this policy prior to being authorized to use the facial recognition system.

4. The Detroit Police Department is guided by applicable laws, regulations, and standards to ensure that privacy, civil rights, and civil liberties are not violated by this facial recognition policy or by the Department's facial recognition information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

307.5 - 6.2 Weekly Report to the Board of Police Commissioners
The Crime Intelligence Unit shall provide a weekly report to the Board of Police Commissioners with information pertaining to the number of facial recognition requests that were fulfilled, the crimes that the facial recognition requests were attempting to solve, and the number of leads produced from the facial recognition software. During this report, if there are any upgrades to the facial recognition software, any planned changes to the contract, and/or any confirmed policy violations, the Department shall notify the Board of Police Commissioners.

307.5 - 6.3 Annual Report to the Board of Police Commissioners
The Crime Intelligence Unit shall provide an annual report to the Board of Police Commissioners. This annual report shall include a summary of the weekly reports and an evaluation of the efficacy of the Department's facial recognition technology. The evaluation shall include if there were any relevant lawsuits or settlements involving facial recognition, the number of cases that use of the technology assisted in investigations, and any other relevant factors. This shall be disseminated at the Board of Police Commissioners' meeting, and electronic copy shall be provided to the Board for dissemination to the public.

307.5 - 6.4 All Policy Changes to the Board of Police Commissioners
The Department shall seek the Board of Police Commissioners' approval regarding any and all changes to the Facial Recognition Policy.

307.5 - 7 Security and Maintenance

1. The Detroit Police Department will comply with generally accepted industry or other applicable standards for security to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related Department activity. The Department's facial recognition system will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to the Department's facial recognition information from outside the facility will be allowed only over secure networks. All results produced by the Department as a result of a facial recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee. When such non-electronic dissemination is made, the member shall memorialize the dissemination as follows:

    a. To whom it was released;
    b. Date and time it was released; and

c. Manner in which it was released (i.e. if by phone, include the number; if in person, include name of witness who saw it released).

2. All members with access to the Department's information or information systems will report a suspected or confirmed breach to their immediate supervisor who will ensure that the local agency security officer (LASO), assigned to Technical Services, is notified as soon as possible without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electric. Following assessment of the suspected or confirmed breach and as soon as practicable, the Department will notify the originating agency from which the entity received facial recognition information of the nature and scope of a suspected or confirmed breach of such information. The Department will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.
3. All facial recognition equipment and facial recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.
4. The Department will store facial recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by members authorized to take such actions.
5. Authorized access to the Department's facial recognition system will be granted only to members whose positions and job duties require such access and who have successfully completed a background check and required training.
6. Usernames and passwords to the facial recognition system are not transferrable, must not be shared by Department members, and must be kept confidential.
7. The system administrator (Department LASO) will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfacial of the system become operational. User passwords must meet the standards outlined in Manual Directive 307.4, Criminal Justice Information Systems (CJIS).
8. Queries made to the Department's facial recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.
9. The Department will maintain an audit trail of requested, accessed, searched, or disseminated facial recognition information. An audit trail will be kept for a minimum of one (1) year of requests, access, and searches of facial recognition information for specific purposes and of what facial recognition information is disseminated to each individual in response to the request. Audit logs will include:

   a. The name and unit of the law enforcement user;
   b. The date of access;
   c. Case number; and

d. The authorized law enforcement or public safety justification for access including a relevant case number.

Series	Effective Date	Review Date	Directive Number
300 Support Services		Annually	307.5
Chapter 307 – Information System			
Reviewing Office Crime Intelligence			☒ New Directive ☐ Revised
References:			

FACIAL RECOGNITION

307.5 - 1 PURPOSE

The purpose of this policy is to establish acceptable use for the Detroit Police Department's (DPD) facial recognition software. Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active or ongoing Part 1 Violent Crime investigation or a Home Invasion I investigation. If a match is found through DPD's Facial Recognition Process, it shall be considered an investigative lead, and the requesting investigator shall continue to conduct a thorough and comprehensive investigation.

307.5 - 2 Definitions

307.5 - 2.1 Biometric Data

Data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and facial recognition data.

307.5 - 2.2 DataWorksPlus

The facial recognition software with which the Department has a contract.

307.5 - 2.3 Examiner

An individual who has received advanced training in the facial recognition system and its features. Examiners have at least a working knowledge of the limitations of facial recognition and the ability to use image editing software. They are qualified to assess image quality and appropriateness for facial recognition searches and to perform one-to-many and one-to-one facial image comparisons.

307.5 - 2.4 Facial Recognition (FR)

The automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity. All Facial Recognition searches must be corroborated by at least two examiners and one supervisor.

307.5 - 2.5 Highly Restricted Personal Information
An individual's photograph or image, social security number, digitized signature, medical and disability information.

307.5 - 2.6 Home Invasion I
Unlawful entry of a dwelling with intent to commit or committing a felony, larceny, or assault on the home when either the unlawful entrant is armed with a dangerous weapon or when another person is lawfully present in the dwelling.

307.5 - 2.7 Part 1 Violent Crimes
~~Part 1 Viole~~For the purposes of this directive, Part 1 Violent Crimes are defined as ~~murder, attempted murder, robbery, carjacking~~robbery, sexual assault, aggravated assault, or homicide, ~~kidnapping, a felonious assault resulting in injury to the victim, and criminal sexual conduct 1st and 3rd degrees~~.

~~nt Crimes include Criminal Homicide, Rape, and Aggravated Assault.~~

307.5 - 2.8 Personally Identifiable Information (PII)
Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

307.5 - 2.9 Reasonable Suspicion
The specific facts and reasonable inferences drawn from those facts to convince an ordinarily prudent person that criminality is at hand.

307.5 - 2.10 Statewide Network of Agency Photos (SNAP)
A computer application managed by the SNAP Unit, deployed through the Michigan Criminal Justice Information Network (MiCJIN) portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

~~307.5 - 2~~307.5 - 3 Prohibited Uses

~~307.5 - 2.1~~307.5 - 3.1 Surveillance
Members shall not use facial recognition ~~software~~ to surveil the public through any camera or video device.

~~307.5 - 2.2~~307.5 - 3.2 Live Streaming or Recorded Videos
Members shall not use facial recognition ~~software~~ on live stream or on recorded videos. This prohibition applies to all videos, whether they originate from DPD itself, from private citizens, or from any other source.

307.5 Facial Recognition

307.5 - 3.3 Mobile Facial Recognition
Members shall not use mobile facial recognition.

307.5 - 3.4 Predictive Analysis
Members shall not use facial recognition for predictive analysis.

~~307.5 - 2.3~~307.5 - 3.5 First Amendment Events
The Detroit Police Department will not violate First, Fourth, and Fourteenth Amendments and will not perform or request facial recognition searches about individuals or organizations based solely on the following:

a. Their religious, political, or social views or activities;
b. Their participation in a particular noncriminal organization or lawful event; or
c. Their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

307.5 - 3.6 Facial Recognition Use for Immigration Enforcement
DPD members are strictly prohibited from using ~~F~~facial ~~R~~recognition to assess immigration status.

~~307.5 - 3~~307.5 - 4 Discipline
Any violations to this policy shall be deemed major misconduct. Any misuse of the facial recognition software will be investigated and reviewed for criminality. The remedy for this misconduct is dismissal from DPD.

If facial recognition is used contrary to section 307.5 -3.5 First Amendment Events, DPD shall notify the Board of Policy Commissioners, the Mayor of Detroit, City Council President, and City Council President Pro Tem within 24 hours of the violation.

~~307.5 - 4~~307.5 - 5 Use of Facial Recognition Technology
~~307.5 - 4.1~~307.5 - 5.1 Use Limited to Still Images
Facial recognition software may only be used on a still image of an individual.

~~307.5 - 4.2~~307.5 - 5.2 Criminal Investigation Required
Members shall not use facial recognition technology unless that technology is in support of an active or ongoing Part 1 Violent Crime investigation (e.g. robbery, sexual assault, or homicide) or a Home Invasion 1 investigation.

307.5 Facial Recognition

~~307.5 - 4.3~~307.5 - 5.3 Individualized Targeting

Members shall not use facial recognition technology on any person unless there is reasonable suspicion that such use of facial recognition technology will provide information relevant to an active or ongoing Part 1 Violent Crime investigation or a Home Invasion I investigation.

~~307.5 - 4.4~~307.5 - 5.4 Process for Requesting Facial Recognition

1. Requests for facial recognition services shall be submitted to the Crime Intelligence Unit (CIU), with photograph(s) to be reviewed, the incident number, the crime type, and other pertinent information. Photographs shall be handled as specified in Manual Directive 306.1 Evidence Property.
2. CIU shall perform facial recognition searches utilizing the Statewide Network of Agency Photos (SNAP) which include criminal mug shot images. In the event additional analysis is needed for confirmation of an investigative lead, a formal request may be made to MSP to search the state's database. Any such request must be approved by a CIU supervisor.
3. If the examiner detects an investigative lead, the examiner must corroborate this lead with at least one other examiner and a CIU supervisor. The corroboration must have written sign-off by the supervisor and all examiners' involved.
4. Upon final approval, CIU shall complete a supplemental incident report for the requestor. The supplemental incident report shall detail how the examiner came to their conclusion, and include the following language:
    4.a. "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigation and investigative resources."
5. In the event that a viable candidate cannot be located, the requestor will be notified that no candidate was identified.
6. If CIU cannot discern a viable candidate, the photograph of the suspect will be ~~purged~~ removed from the facial recognition system.

307.5 - 5.5 Outside Agency Using Facial Recognition

An outside agency, or investigators from an outside agency, may request searches to assist with investigations only if the following requirements are met:

a. Prior to making the request, the outside agency has a formalized agreement (e.g. a memorandum of understanding or an interagency agreement) between the Detroit Police Department and the outside agency;
b. The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in this directive and the requestor provides a case number and contact information

(requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:

- "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigation and investigative resources."

c. If any agency is found not in compliance with this Directive, the Department shall immediately suspend all Facial Recognition requests until the requesting agency becomes in compliance with this Directive.

~~6.~~

~~307.5 - 5~~307.5 - 6 Governance and Oversight

307.5 - 6.1 LASO & Crime Intel Responsibilities

1. The primary responsibility for the operation of the Department's criminal justice information systems, facial recognition program and system, operations, and the coordination of personnel, the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Local Agency Security Officer (LASO) who is assigned to Technical Services.

~~307.5 - 5.1 Report to the Board of Police Commissioners~~

~~DPD shall provide a weekly report to the Board of Police Commissioners with information pertaining to the number of facial recognition requests that were fulfilled, the crimes that the facial recognition requests were attempting to solve, and the number of leads produced from the facial recognition software.~~

2. The LASO will be responsible for the following:

   a. Overseeing and administering the facial recognition program to ensure compliance with applicable laws, regulations, standards, and policy;
   b. Acting as the authorizing official for individual access to facial recognition information;
   c. Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status; and
   d. Ensuring that random evaluations of user compliance with system requirements along with this policy and applicable laws are conducted and documented;

3. The commanding officer of the Crime Intelligence Unit will be responsible for the following:

a. Reviewing facial recognition search requests, reviewing the results of facial recognition searches, and returning the most likely candidates – or candidate images – if any, to the requestor.
b. Ensuring that protocols are followed to ensure that facial recognition information (including probe images) is automatically purged in accordance with this Department's retention policy, unless determined to be of evidentiary value;
c. Confirming, through random audits, that facial recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy; and
d. Ensuring and documenting that personnel (including investigators from external agencies who request facial recognition searches) meet all prerequisites stated in this policy prior to being authorized to use the facial recognition system.

4. The Detroit Police Department is guided by applicable laws, regulations, and standards to ensure that privacy, civil rights, and civil liberties are not violated by this facial recognition policy or by the Department's facial recognition information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

307.5 - 6.2 Weekly Report to the Board of Police Commissioners

The Crime Intelligence Unit shall provide a weekly report to the Board of Police Commissioners with information pertaining to the number of facial recognition requests that were fulfilled, the crimes that the facial recognition requests were attempting to solve, and the number of leads produced from the facial recognition software. During this report, if there are any upgrades to the facial recognition software, any planned changes to the contract, and/or any confirmed policy violations, the Department shall notify the Board of Police Commissioners.

307.5 - 6.3 Annual Report to the Board of Police Commissioners

The Crime Intelligence Unit shall provide an annual report to the Board of Police Commissioners. This annual report shall include a summary of the weekly reports and an evaluation of the efficacy of the Department's facial recognition technology. The evaluation shall include if there were any relevant lawsuits or settlements involving facial recognition, the number of cases that use of the technology assisted in ~~closing cases~~investigations, and any other relevant factors. This shall be disseminated at the Board of Police Commissioners' meeting, and electronic copy shall be provided to the Board for dissemination to the public.

307.5 - 6.4 All Policy Changes to the Board of Police Commissioners

The Department shall seek the Board of Police Commissioners' approval regarding any and all changes to the Facial Recognition Policy.

307.5 - 7 Security and Maintenance

1. The Detroit Police Department will comply with generally accepted industry or other applicable standards for security to protect data at rest, in motion, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related Department activity. The Department's facial recognition system will operate in a secure facility protected with multiple layers of physical security from external intrusion and will utilize secure internal and external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to the Department's facial recognition information from outside the facility will be allowed only over secure networks. All results produced by the Department as a result of a facial recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee. When such non-electronic dissemination is made, the member shall memorialize the dissemination as follows:

    a. To whom it was released;
    b. Date and time it was released; and
    c. Manner in which it was released (i.e. if by phone, include the number; if in person, include name of witness who saw it released).

2. All members with access to the Department's information or information systems will report a suspected or confirmed breach to their immediate supervisor who will ensure that the local agency security officer (LASO), assigned to Technical Services, is notified as soon as possible without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electric. Following assessment of the suspected or confirmed breach and as soon as practicable, the Department will notify the originating agency from which the entity received facial recognition information of the nature and scope of a suspected or confirmed breach of such information. The Department will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.
3. All facial recognition equipment and facial recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.
4. The Department will store facial recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by members authorized to take such actions.

307.5 Facial Recognition

5. Authorized access to the Department's facial recognition system will be granted only to members whose positions and job duties require such access and who have successfully completed a background check and required training.
6. Usernames and passwords to the facial recognition system are not transferrable, must not be shared by Department members, and must be kept confidential.
7. The system administrator (Department LASO) will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfacial of the system become operational. User passwords must meet the standards outlined in Manual Directive 307.4, Criminal Justice Information Systems (CJIS).
8. Queries made to the Department's facial recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.
9. The Department will maintain an audit trail of requested, accessed, searched, or disseminated facial recognition information. An audit trail will be kept for a minimum of one (1) year of requests, access, and searches of facial recognition information for specific purposes and of what facial recognition information is disseminated to each individual in response to the request. Audit logs will include:

   a. The name and unit ~~e, unit, and contact information~~ of the law enforcement user;
   b. The date ~~and time~~ of access;
   c. Case number; and
   ~~Probe images;~~
   ~~The specific information accessed;~~
   ~~The modification or deletion, if any, of the facial recognition information; and~~
   The authorized law enforcement or public safety justification for access including a relevant case number.
   d.

Board of Police Commissioners' Policy Recommendations for Facial Recognition
Proposed Policy 307.5

Below, DPD reproduced the Board of Police Commissioners' recommendations, and added DPD's response to each recommendation.

Broad Category: Addresses Key Administrative Recommendations and general areas of importance.

BOPC Recommendation #1: Specify the purpose of the Facial Recognition Technology's permitted use. The Department shall specify the purpose of the Facial Recognition Technology's permitted limited use.

a. See below for an example from Georgetown Law
    i. "Face recognition refers to an automated process of matching face images, utilizing algorithms and biometric scanning technologies [and human component review]."
    ii. The system aids in the support of an ongoing Part 1 violent crime investigation or a home invasion I investigation.
    iii. Part 1 Violent Crimes: Criminal homicides, sexual assaults, aggravated assaults, non-fatal shootings, robberies, and carjackings
    iv. Home Invasion I Elements
        1. Entered a home without permission or broke in
        2. Intended to commit or did commit a felony, larceny, or assault in the home, and
        3. Either was armed with a dangerous weapon or entered while another person was lawfully within the home.
        4. See MCL 750.110a(2)
    v. The use of the Facial Recognition Technology is only utilized to identify investigative leads. The requesting investigator shall continue to conduct a thorough and comprehensive investigation.

DPD Response: DPD expanded its purpose section for clearer articulation of how Facial Recognition would be used within the department. For items I – IV, DPD added definitions; however, the Department did not want to add all of these items within the purpose as to create an unreasonably long purpose statement.

BOPC Recommendation #2: Required Facial Recognition Technology Training: The Department shall indicate that Department members utilizing the Facial Recognition technology system shall have ongoing, competent training from an experienced source to access and operate the Facial Recognition Technology software (ie FBI Agency, Department-approved training, and other national recognized Facial Recognition conferences, etc.).

DPD Response: DPD added a definition for the "Examiner" in 307.5 – 2.3 stating that an examiner is "An individual who has received advanced training in the facial recognition system and its features. Examiners have at least a working knowledge of the limitations of facial recognition and the ability to use image editing software. They are qualified to assess image

quality and appropriateness for facial recognition searches and to perform one-to-many and one-to-one facial image comparisons."

BOPC Recommendation #3: Specify Supervisor Responsibilities: The Department shall specify the Crime Intelligence Unit Supervisor's responsibilities within the proposed policy directive (i.e. Supervisory Review of all Peer-to-Peer evaluations, written evaluation required for each review, monitoring use of system, etc).

DPD Response: DPD stipulated with 307.5 - 5.4 (3) that supervisors must confirm any potential investigative lead. In addition, the Department added that there must be written sign-off for any investigative lead by a supervisor. Further responsibilities can be found within 307.5 – 6 Governance and Oversight.

BOPC Recommendation #4: Indicate Minimum Standard. The Department shall specify the minimum threshold standard at the beginning of the policy directive for the use of the Facial Recognition Technology. (also noted within the definition standard."

a) I.e. Reasonable Suspicion – defined as 'specific articulable facts coupled with rational inferences when taken together that reasonably warrant the degree of intrusion' or
b) Heightened standard: Probable Cause: 'A reasonable belief that a person has committed, is committing, or will commit a crime.'

DPD Response: DPD added this within the purpose. The Purpose now includes the following text: "Facial Recognition technology shall only be used when there is reasonable suspicion that such use will provide information relevant to an active or ongoing Part 1 Violent Crime investigation or a Home Invasion I investigation. Any such match found through DPD's Facial Recognition Process shall be considered an investigative lead, and the requesting investigator shall continue to conduct a thorough and comprehensive investigation."

BOPC Recommendation #5: Include Definitions for public and operational clarity. The Department shall retain the terms initially identified in the first proposed policy on Facial Recognition, which are as follows:

a) Biomentric Data
b) DataWorks Plus
c) Facial Recognition
d) Certified Examiner
e) Highly Restricted Personal Information
f) Personally Identifiable Information
g) Statewide Network of Agency Photos (SNAP)
h) Talon System

The Department shall also define the following terms within Department Policy:

a) Reasonable Suspicion – define and cite which level of standard is allowed for use of the Facial Recognition System
b) Probable Cause – Define and cite which level of standard is allowed for use of the facial recognition system
c) Part 1 Violent Crimes
d) Home Invasion 1 Elements

e) Authorized User – an individual who is authorized to access the SNAP application and whose agency is approved by the Detroit Police Department and the Michigan Department of State (MSP) to utilize the SNAP
f) Probe Image – Biometric characteristics obtained at the site of verification or identification submitted through an algorithm which converts the characteristic into biometric features for comparison with biometric templates.
g) Participating Agencies – please specify all participating agencies within the Department policy
h) Identification – a task where the biometric system searches a database for a biometric template that matches a submitted biometric sample (probe), and if found, returns a corresponding identity

Please site whether the following terms will be applicable regarding the use of facial recognition system:

a) False Negative: An incorrect non-match between a probe and a cadndiate in the gallery returned by a face recognition algorithm, technology, or system.
b) False Positive: An incorrect match between a biometric probe and biometric template returned by a face recognition during the verification task.
c) False Reject: An incorrect non-match between a biometric probe and biometric template returned by a face recognition during the verification task.
d) False Reject Rate: A statistic used to measure biometric performance when performing the verification task. The percentage of times a facial recognition algorithm, technology, or system incorrectly rejects a true claim to existence or non-existence of a match in the gallery, based on the comparison of a biometric probe and biometric template.
e) Identification: A task where the biometric system searches the database for a biometric template that matches a submitted biometric sample (probe), and if found, returns a corresponding identity.

DPD RESPONSE: DPD added all definitions relevant to the policy. DPD did not add "Talon System", "Authorized User", "Probe Image", "Participating Agencies", and "Identification", because these terms do not arise in the new policy. The Examiner is the only authorized user, and DPD added a definition for the examiner within the policy. Participating agencies is discussed in 307.5 – 5.5.

The last series of definitions is not relevant to DPD policy, because DPD does not use any of the computer-generated results without the Examiner analyzing the matches; thus, the Department cannot track the software's rates discussed in A-E.

BOPC Recommendation #6: Address Data Retention Area. The Department shall address any applicable Data Retention Requirements within the proposed directive.

a) Ie The Department shall be prohibited from retaining a separate Facial Recognition Database for any purpose. (i.e. retaining those photo images not identified as investigative leads).

DPD RESPONSE: This was already within the policy under 307.5 -5.4 (6).

BOPC Recommendation #7: Prevention against hacking and other data breaches: The Department shall implement preventative and remedial measures regarding data collection

protection and maintenance for Facial Technology Use. The Department shall retain specific measures in an internal training document consistent with the Department's current policy on data protection and security. The Department shall add a provision confirming that it will prevent data breaches and protect confidential and sensitive information.

DPD RESPONSE: DPD added section 307.5 – 7 "Security and Maintenance" to address this recommendation.

BOPC Recommendation #8: Requesting Procedures: The Department shall add the following provision as contained in the initial proposed Facial Recognition policy: Under 307.5 – 6 Section 2, it states the following: 'Requests for facial recognition services shall be submitted, through channels, on an Inter-Office Memorandum (DPD 568) to the commanding officer of Crime Intelligence with photographs, or videos to be reviewed. Photographs and videos shall be handled as specified in Manual Directive 306.1 Evidence Property."

a) Additional recommendations for 'Process for Requesting Facial Recognition':
   i. Spell out the names of other image depositories
   ii. Review the sequencing of these tasks to determine whether the order should be reconsidered.
   iii. Add 'and not to be added to another image file controlled or shared by or with DPD or another law enforcement agency. Purged- should mean destroyed – not retained.'
   iv. The CIU shall keep a current log of all usage and individuals accessing the facial recognition software. The log shall be reviewed weekly by Command supervision. The logs shall be made available upon request for review and inspection by the Board of Police Commissioners.

DPD Response: Please see below for a response to each response:

8: The process is no longer done through a 568, which is why it was removed from the policy. DPD added Photographs shall be handled as specified in Manual Directive 306.1 Evidence Property in 307.5 5.4 (1).

i. DPD has listed the image repositories in section 307.5 – 5.4 Process for Requesting Facial Recognition (2): "CIU shall perform facial recognition searches utilizing the Statewide Network of Agency Photos (SNAP) which include criminal mug shot images. In the event additional analysis is needed for confirmation of an investigative lead, a formal request may be made to MSP to search the state's database. Any such request must be approved by a CIU supervisor."
ii. The order is correct.
iii. Within 307.5 – 5.4 (6), DPD used the word "purged" to mean remove. DPD changed purged to remove to clarify any potential confusion. DPD cannot 'destroy' a picture of a suspect if the investigation is ongoing irrespective of if the facial recognition system identified a match.
iv. DPD added Section 307.5 – 7 (9) to address the above concern.

BOPC Recommendation #9: Notification regarding Data Works Plus Contract Proposals, Grants, and Other Modifications, etc.: The Department shall immediately inform the Board of Police Commissioners in writing and during the next immediate schedule Board of Police Commissioners' Meeting of any current or future plans of Facial Recognition technology customizing contract proposals, changes, or varying use. (i.e. addition, deletion, extension or modification of the contract, etc. Additionally, the Department shall provide the Board of Police Commissioners with a copy of any proposed or existing grants related to Facial Recognition or any other advanced technology. The Department shall also provide the Board of Police Commissioners with the updated Data Works Plus Contract.

DPD Response: DPD added within the Definitions Section (307.5 – 2.2) that Data Works Plus is the current Facial Recognition software vendor. If any change occurs in regard to vendor, DPD shall update the policy and submit it to review to the Board. Also, DPD has added the following under Section 307.5 – 6.2: "During this report, if there are any upgrades to the facial recognition software, any planned changes to the contract, and/or any confirmed policy violations, the Department shall notify the Board of Police Commissioners."

BOPC Recommendation #10: Notification of Changes to Facial Recognition Department Policy: The Department shall seek the Board of Police Commissioners' approval regarding any and all changes to the Facial Recognition Policy. Examples include but are not limited to the following: Consideration of expansion of technology, functionality use, or change(s) regarding system.

DPD Response: The Department shall seek the Board of Police Commissioners' approval regarding any and all changes to the Facial Recognition Policy.

BOPC Recommendation #11: Notification of Algorithm Agnostic Upgrade, Improvements, or Changes: The Department shall immediately notify the Board of all algorithm agnostic upgrades improvements, or changes with the Facial Recognition System.

DPD Response: DPD has added the following under Section 307.5 – 6.2: "During this report, if there are any upgrades to the facial recognition software, any planned changes to the contract, and/or any confirmed policy violations, the Department shall notify the Board of Police Commissioners."

BOPC Recommendation #12: Notification of Policy Violations including any Breach of First Amendment Violations 307.5 – 5.2. The Department shall add the following provision: 'if for any reason facial recognition is used contrary to Department Policies and procedures including but not limited to Section 307.5 – 2.3 (First Amendment Events), the Board of Police Commissioners, the Mayor, City Council President, and President Pro Tem shall be notified within 4 hours of a breach. Notification shall be both verbally and written."

DPD Response: DPD has added the following under Section 307.5 – 6.2: "During this report, if there are any upgrades to the facial recognition software, any planned changes to the contract, and/or any confirmed policy violations, the Department shall notify the Board of Police Commissioners." Further, DPD added the following section with 307.5 – 4 If facial recognition is used contrary to section 307.5 -3.5 First Amendment Events, DPD shall notify the Board of Policy Commissioners, the Mayor of Detroit, City Council President, and President Pro Tem within 24 hours of the violation.

BOPC Recommendation #13: Provide Clarity Regarding Outside Law Enforcement Agencies Required Adherence to Department Policy: The Department shall specify that any law enforcement agency granted access or permissive use of the Facial Recognition System shall adhere to the Detroit Police Department's policy guidelines. Additionally, the Department shall document in writing its approval for outside agencies' use or access to the Facial Recognition System, and immediately notify the Board of Police Commissioners."

DPD Response: DPD added Section 307.5 5-5 Outside Agency Using Facial Recognition stating " An outside agency, or investigators from an outside agency, may request searches to assist with investigations only if the following requirements are met:

a) Prior to making the request, the outside agency has a formalized agreement (e.g. a memorandum of understanding or an interagency agreement) between the Detroit Police Department and the outside agency;

b) The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in this directive and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:

"The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigation and investigative resources."

BOPC Recommendation #14: Facial Recognition Review Requiring Written Documentation of Concurrence or Disagreement of Review. Under Section 307.5 – 4.4 Process for Requesting Facial Recognition, subsections 4 & 6: For accountability and transparency measures, the Facial Recognition Examiner, Peer Reviewer(s), and CIU Supervisor shall each document in writing their individual concurrence or disagreement within the supplemental report for the requesting investigator or the specific report prepared when no viable candidate is identified.

DPD Response: DPD added the following to 307.5 – 5.4 (3) "If the examiner detects an investigative lead, the examiner must corroborate this lead with at least one other examiner and a CIU supervisor. The corroboration must have written sign-off by the supervisor and all examiners' involved." The supervisor does not have to review a supplemental report that does not have an investigative lead.

BOPC Recommendation #15: Required Department Audits: The Department shall include within Department policy that it is engaged in continuous internal auditing processes. Additionally, the Department shall provide the Board of Police Commissioners with its internal auditing processes and reports of conclusions on an annual basis or as determined by the Board of Police Commissioners.

- Such information shall address the following but not be limited to the following: Whether the auditing process include inspections for accuracy and racial bias as well as inspections regarding trained face examiners' activities?
- Whether the Department allows a third party agency to conduct the auditing?
- Whether the Department will engage in its own auditing measures? What will be the processes?
- The percentage rate of identifying Part 1 Violent Crime offenders.

DPD Response: DPD has inputted information pertaining to audits with section 307.5 – 6.1 LASO & Crime Intel Responsibilities (3b) & 307.5 -7 Security and Maintenance. More detailed information pertaining to how the audit will be conducted is more appropriate for the Standard Operating Procedure than a Policy Directive.

BOPC Recommendation #16: Enforcement Provisions: The Department shall add the Enforcement Provisions as identified in the initial proposed draft policy under Section 306.5 – 8.3. The provision reads as follows: "Any authorized user who is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging may be subject to the following:

a) Suspend or discontinue access to information
b) Apply appropriate disciplinary or administrative actions or sanctions; and/or
c) Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy;
d) The Department reserves the right to establish the qualifications and number of personnel having access to the Department's facial recognition system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this facial recognition policy
e) The department shall immediately inform the Board of Police Commissioners in writing of all enforcement actions and alleged offending personnel involved.

DPD Response: DPD discusses A – C in section 307.5 – 4. In addition, DPD added 307.5 – 5.5 (c) to discuss noncompliant requesting agencies.

BOPC Recommendation #17: <u>Specify Annual Report Mandatory Provisions 307.5 – 5.3</u>: The Department shall add the following provision under 307.5 – 5 Governance and Oversight: "The Department (DPD) shall develop a separate annual report on the use of Facial Recognition utilization outlining its use, results, and effectiveness in investigating and solving crime. The report shall include if a warrant request was obtained from any prosecutorial authorities. The report is intended to track and discuss the long term effects of the use of the technology that would not normally appear in segregated weekly reports. The report should also make a determination if Facial Recognition, based on the actual experience with Facial Recognition technology, is useful for the Department. Such determination will also weigh the current and future costs of the technology as one determining factor to continue the use. The Report shall also include information on the type and amount of legal judgement settlements and lawsuits wherein Facial Recognition technology was shown to be a liability in whole or in part in financial payout by the City.

Such Annual Report shall be completed and transmitted to the appropriate agencies by the close of each fiscal year with copies provided to the Board of Police Commissioners, the Detroit

City Council, Mayor of the City of Detroit, the Clerk for the City of Detroit and a list of civil right organizations including but not limited to the Damon J. Keith Law Center (Wayne State University), American Civil Liberties Union (ACLU), Detroit Digital Project, NAACP, and the Urban League. The Annual Report shall also be published on the website of the City of Detroit, Board of Police Commissioners, and Detroit Police Department for public access.

DPD RESPONSE: DPD added the following to 307.5 – 6.3 "The Crime Intelligence Unit shall provide an annual report to the Board of Police Commissioners. This annual report shall include a summary of the weekly reports and an evaluation of the efficacy of the Department's facial recognition technology. The evaluation shall include if there were any relevant lawsuits or settlements involving facial recognition, the number of cases that use of the technology assisted in investigations, and any other relevant factors. This shall be disseminated at the Board of Police Commissioners' meeting, and electronic copy shall be provided to the Board for dissemination to the public."

BOPC Recommendation #18: Require Compliance with Laws: The Department shall comply with current federal, state, and local laws. Further Department Policy should require yearly checks and compliance with all applicable laws to anticipate new regulations.

DPD RESPONSE: Please refer to 101.1 – 3 Legal Advisor Updates: "The purpose of Legal Advisor Updates is to review court decisions and changes to the law that may affect this department. They are numbered sequentially and shall be permanently retained by all members until revoked or until the periodic index indicates that they shall be deleted."

BOPC Recommendation #19: Indicate in Department Policy that Facial Recognition Technology Does Not Establish Probable Cause to Arrest: The Department shall specify that the Facial Recognition Image Result does not establish probable cause for an arrest and shall only be used as an investigative lead in Part I Violent Crime investigations and Home Invasion I investigations.

A. Recommended language: "The Facial Recognition Information provided does not constitute probable case for an arrest. The results are only possible names of the photograph(s) and video(s) that were submitted with the request. It shall be the responsibility of the assigned detective to verify the identity of all suspects."

1. **DPD Response**: DPD added the following language in 307.5 – 5.4 (4): The supplemental incident report shall detail how the examiner came to their conclusion, and include the following language:
    - "The result of a facial recognition search is provided by the Detroit Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigation and investigative resources."

BOPC Recommendation #20: Prohibition against mobile facial recognition, live stream, real time, or any other constant streaming video using drones, etc.: The Department shall be prohibited from using Facial Recognition through the use of Mobile FR/Evolution Multimodal Identification Device, live video using drones, etc.

DPD Response: DPD identifies that there will be no facial recognition conducted on live streaming or recorded video. In addition, DPD added 307.5 – 3.3 Mobile Facial Recognition stating that "Members shall not use mobile facial recognition software."

BOPC Recommendation #21: Prohibition against facial recognition for immigration purposes: The DPD shall be prohibited from the use of Facial Recognition from Immigration Enforcement purposes. The DPD shall also be prohibited from allowing or sharing Facial Recognition photographs or information with the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE), Customs and Border Patrol, or any other agency involved in immigration enforcement measures.

DPD Response: DPD added section 307.5 – 3.5 Facial Recognition Use for Immigration Enforcement stating "DPD members are strictly prohibited from using Facial Recognition to assess immigration status." In addition, DPD added the following section concerning outside agency requests for facial recognition: "The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in this directive"

BOPC Recommendation #22: Predictive Analytics Prohibited. The Department shall be prohibited from using Predictive Analytics through the use of Facial Recognition Technology. Predictive analytics is the branch of the advanced analytics, which is used to make predictions about unknown future events. Predictive analytics uses many techniques from data mining, statistics, modeling, machine learning, and artificial intelligence to analyze current data to make predictions about the future.

DPD Response: DPD added the following section 307.5 - 3.4 Predictive Analysis stating "Members shall not use facial recognition software for predictive analysis."

BOPC Recommendation #23: Reemphasize Guarantee of Constitutional Protections. The Department shall not violate First, Fourth, Fourteenth Amendments and will not perform or request facial recognition searches against individuals or organizations based on the following

- Prohibition: First amendment violations (religion, freedom of expression and association, political (i.e. Red Files), and social activities and events)
- Prohibition: Fourth amendment violations (illegal searches and seizures)
- Prohibition: Fourteenth Amendment Violations (profiling against selected classes (ie race, gender identification, sex, religion, immigration status, sexual orientation, disabilities, age discrimination, places of origins, and other classes protected by law."

DPD Response: Please see section 307.5 – 3.4 307.5 - 3.4 First Amendment Events

"The Detroit Police Department will not violate First, Fourth, and Fourteenth Amendments and will not perform or request facial recognition searches about individuals or organizations based solely on the following:

a. Their religious, political, or social views or activities;

b. Their participation in a particular noncriminal organization or lawful event; or

c. Their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law."