AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND

3600 CLIPPER MILL ROAD
SUITE 200
BALTIMORE, MD 21211
T/410-889-8555
F/410-366-7838

WWW.ACLU-MD.ORG

OFFICERS AND DIRECTORS
COREY STOTTLEMYER
PRESIDENT

DANA VICKERS SHELLEY
EXECUTIVE DIRECTOR

ANDREW FREEMAN
GENERAL COUNSEL

VIA EMAIL

Phillip M. Pickus
Principal Counsel
Maryland State Police
Legal Counsel Section
1201 Reisterstown Road
Pikesville, MD 21208-3899

Dear Mr. Pickus,

The ACLU of Maryland writes regarding the requirement, recently enacted as part of Senate Bill 182,[1] that the Department of State Police "shall adopt and publish a model statewide policy regarding the use of facial recognition technology." Md. Code Ann., Crim. Proc. § 2-506(a). Maryland law enforcement agencies will be required to comply with this model statewide policy if they wish to use the technology. *Id.* § 2-506(b).

As explained in detail below, we urge you to ensure that the following baseline protections are incorporated into the model statewide policy on facial recognition technology (FRT):

- A photographic lineup or similar identification procedure cannot constitute sufficient "additional, independently obtained evidence establishing probable cause or a positive identification" required by S.B. 182 because false matches generated by FRT searches will often look so much like the actual suspect as to taint the reliability of a subsequent lineup or other identification procedure.

- Prohibit use of FRT to identify or track individuals through analysis of both live and recorded video.

[1] S.B. 182, 2024 Md. Laws Ch. 808, to be codified at Md. Code, Crim. Proc. §§ 2-501–510, https://mgaleg.maryland.gov/2024RS/Chapters_noln/CH_808_sb0182e.pdf.

- Prohibit use of private third-party FRT matching databases that consist of images, or faceprints extracted from those images, that were collected illegally or without consent.

As you are no doubt aware, law enforcement use of facial recognition technology (FRT) poses significant risks. The technology often generates false matches (and when it produces multiple potential matches for a human to review *always* produces matches that are false, because by definition only one can be the actual match), and has contributed to at least seven known wrongful arrests across the country, including at least one in Maryland.[2] Numerous studies, including from the National Institute of Standards and Technology, demonstrate that the false match rates of this technology are significantly higher when it is used to attempt to identify people of color and women.[3] Indeed, nearly all of the known cases of wrongful arrests due to police reliance on incorrect FRT results have involved the arrests of Black people. And even aside from the significant accuracy problems, deployment of FRT threatens to enable mass surveillance by the government that would violate bedrock constitutional protections.

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND

In recognition of the twin dangers of racially disparate false identifications and pervasive surveillance, more than 20 jurisdictions across the country, from Pittsburgh, to Austin, to San Francisco, to the State of Vermont, have enacted bans on law enforcement use of FRT. The ACLU agrees that facial recognition technology is inappropriate for law enforcement use due to these documented dangers. Nonetheless, in light of the recent enactment of legislation regulating and constraining law enforcement use of FRT in Maryland, we write to offer input on minimum protections necessary to safeguard Maryland residents and comply with

---

[2] *See generally* Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance. Regarding the wrongful arrest of Maryland resident Alonzo Sawyer by Maryland law enforcement, see Eyal Press, *Does A.I. Lead Police to Ignore Contradictory Evidence?*, New Yorker (Nov. 20, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence/; Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, Wired (Feb. 28, 2023), https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/.

[3] *See* Patrick Grother et al., U.S. Dep't of Com., Nat'l Inst. of Standards & Tech., *Face Recognition Vendor Test Part 3: Demographic Effects* 2–3, 8 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. *See also* Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, Wash. Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

the legislature's mandate. These protections will also help avoid uses of FRT that may subject Maryland law enforcement agencies to legal liability for abuse of the technology.[4]

I. A post-FRT photographic lineup or similar identification procedure does not constitute "independently obtained evidence to establish probable cause or a positive identification"

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND

Senate Bill 182 provides that "results generated by facial recognition technology may not serve as the sole basis to establish probable cause or the positive identification of an individual in a criminal investigation or proceeding." Md. Code, Crim. Proc. § 2-502(b)(2)(i). It further requires that "probable cause or positive identification may be established using facial recognition technology only if the results are supported by additional, independently obtained evidence establishing probable cause or a positive identification." *Id.* § 2-502(b)(2)(ii).

It is critical that the Maryland FRT policy clarify what constitutes "additional, independently obtained evidence" in this context. Specifically, the policy should make clear that a lineup or other identification procedure following a FRT search does not constitute independent evidence, because a false FRT match will often bias subsequent human identifications, rendering them unreliable and lacking in independence.

Warnings that FRT results may not serve as the sole basis to establish probable cause or positive identification have long been standard in police department FRT policies and on FRT investigative lead reports provided to police. But without clarification, those warnings are not effective in preventing wrongful arrests. In most of the known cases of wrongful arrests due to police reliance on incorrect FRT results, police received such warning but arrested innocent people nonetheless.[5] A major source of the problem comes when police move directly

---

[4] For example, there are at least six pending or settled lawsuits across the country alleging wrongful arrests due to police reliance on incorrect facial recognition results. *See Parks v. McCormac*, No. 21-cv-04021 (D.N.J.); *Williams v. City of Detroit*, No. 21-cv-10827 (E.D. Mich.); *Oliver v. Bussa*, No. 20-cv-12711 (E.D. Mich.); *Woodruff v. City of Detroit*, No. 23-cv-11886 (E.D. Mich); *Reid v. Bartholomew*, No. 23-cv-4035 (N.D. Ga.); *Murphy v. Essilorluxottica, USA Inc.*, No. 24-cv-801 (S.D. Tex.).

[5] For example, a Detroit Police Department policy adopted in 2019 provided that an FRT result is "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 investigative resources." *See* Detroit Police Dep't, Directive No. 307.5, § 5.4(4) (effective date Sept. 19, 2019) (superseded by 2024 policy update). Nonetheless, just last year Detroit police wrongfully arrested Porcha Woodruff, an eight-months pregnant woman, for a carjacking and armed

from a facial recognition lead to a witness identification procedure, such as a photographic lineup. That is because a false FRT match taints the subsequent identification procedure by introducing an image that looks very similar to the suspect, but is not the suspect. In effect, the FRT search flags an innocent doppelgänger. Because the FRT-selected image is likely to look far more like the actual suspect than any of a lineup's filler photographs, it creates a heightened chance a witness will mistakenly identify the person in the FRT-selected photo as the suspect, even though it is not a true match. As one scholar put it, "[t]he witness's corroboration may be so closely tied to the computerized face-recognition match that it lacks independence."[6]

This problem contributed to the wrongful arrests of Robert Williams, Porcha Woodruff, and Michael Oliver in Michigan, Nijeer Parks in New Jersey, Harvey Eugene Murphy Jr. in Texas, and Alonzo Sawyer here in Maryland. In each case, police obtained an arrest warrant based solely on the combination of a false match from face recognition technology, followed by what turned out to be a false identification by a human. Because that human identification was tainted by the FRT false-match lookalike, it could not in fact constitute independent confirmatory evidence, but officers treated it as if it did.

Model policy language for mitigating this risk can be found in the Detroit Police Department's (DPD) newly updated policies regarding FRT, which were adopted pursuant to a negotiated settlement agreement in the wrongful arrest lawsuit

---

robbery that surveillance footage and witness interviews would have easily established was not conducted by a visibly pregnant perpetrator. However, the only additional investigative step that police did conduct, a photographic lineup, only served to reinforce the incorrect FRT result. *See* Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html. Similarly, the officer responsible for the wrongful arrest of Nijeer Parks in New Jersey was warned that an FRT result "should only be considered an investigative lead. Further investigation is needed to confirm a possible match through other investigative corroborated information and/or evidence. INVESTIGATIVE LEAD, NOT PROBABLE CAUSE TO MAKE AN ARREST." Exhibits to Defs' Motion for Summary Judgment, *Parks v. McCormac*, No. 21-cv-04021 (D.N.J. July 23, 2021), ECF No. 109-5, at 290. The officer responsible for the wrongful arrests of Robert Williams and Michael Oliver in Detroit was warned that an FRT search result "is only 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." Exhibit 5 to Pl's Resp. & Br. in Opp. To Defs' Mot. For Summary J., *Oliver v. Bussa*, No. 20-cv-12711 (E.D. Mich. Apr. 13, 2023), ECF No. 49-5.

[6] Henry H. Perritt Jr., *Defending Face-Recognition Technology (And Defending Against It)*, 25 J. Tech. L. & Pol'y 41, 59 (2021).

brought by Robert Williams.[7] Using the DPD policies as a model, the Maryland FRT policy should specify that:

- A request for an arrest warrant, or an arrest, shall not be made solely on the basis of an investigative lead developed through facial recognition technology in combination with a lineup or other human identification. A request for an arrest warrant, or an arrest, must be supported by additional, independently obtained evidence establishing probable cause or a positive identification.[8]

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND

- Prior to conducting a photographic line-up or other witness identification, a supervisor shall ensure that there is an independent basis supported by reliable evidence that the suspect, who will be presented to the witness, committed the crime. An investigative lead generated by a search using facial recognition technology does not alone constitute an independent basis that the person selected as the lead committed the crime.[9]

Incorporating these protections into the Maryland FRT policy will help ensure that any arrest following an FRT search be justified by evidence that is obtained truly "independently" of the FRT search, as required by Maryland law. *See* Crim. Proc. § 2-502(b)(2)(ii).

II. Prohibit use of facial recognition technology for surveillance of live or recorded video

Senate Bill 182 prohibits the "use of facial recognition technology for the purpose of live or real-time identification of an image or a recording." Crim. Proc. § 2-503(a)(1)(v). This is an important protection, but without further clarification it is vulnerable to circumvention and abuse.

---

[7] *See* Kashmir Hill, *Facial Recognition Led to Wrongful Arrests. So Detroit Is Making Changes.*, N.Y. Times (June 29, 2024), https://www.nytimes.com/2024/06/29/technology/detroit-facial-recognition-false-arrests.html. The full stipulated settlement agreement in *Williams v. City of Detroit*, No. 21-cv-10827 (E.D. Mich.), is attached to this letter and is available at https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest?document=Settlement-Agreement.

[8] *See* Detroit Police Department, Manual Directive No. 307.5 (Facial Recognition), § 5.3, *available as Williams* Settlement Agreement Attachment A, *supra* note 7.

[9] *See* Detroit Police Department, Manual Directive No. 203.11 (Eyewitness Identification and Lineups), § 4.2(3), *available as Williams* Settlement Agreement Attachment C, *supra* note 7.

As the National Academy of Sciences recently explained, "[i]ndiscriminate use of FRT in public and quasi-public places can have significant impacts for privacy and related civil liberties. Indeed, the collection of images in public places that could be subject to FRT may deter people from exercising their civil rights."[10] Deployment of FRT for video analysis, tracking, and surveillance poses a dire threat to privacy, free speech, and freedom of movement, by putting in the hands of government the ability to identify and track anyone or everyone as they go about their daily lives.

AMERICAN CIVIL
LIBERTIES UNION
FOUNDATION OF
MARYLAND

However, a policy that only prohibits use of FRT on "live or real-time" video is too narrow, for two reasons. First, it can be easily circumvented by a minimal delay between collection of video and use of FRT to analyze that video. Arguably, a several-second delay would render the use of FRT no longer "live or real-time," but the concerns raised by near-contemporaneous surveillance are identical to the concerns raised by literally live surveillance.

And second, FRT analysis of recorded video to track individuals' past movements, associations, and activities can be every bit as revealing and intrusive as conducting live FRT surveillance. In *Carpenter v. United States*, for example, the Supreme Court held that government access to a particular individual's historical cell site location information requires a warrant, because of all the "privacies of life" such retrospective tracking can reveal.[11] And as the U.S. Court of Appeals for the Fourth Circuit explained in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, dragnet tracking of people's movements through analysis of recorded wide-area camera footage is an unconstitutional general search.[12]

Indeed, Maryland law already places prohibitions on law enforcement using FRT to search one significant category of recorded video: stored video captured by body worn cameras. The Maryland Police Training and Standard's Commission's Body-worn Camera Policy,[13] which Maryland law enforcement agencies are

---

[10] Nat'l Acad. of Scis., *Facial Recognition: Current Capabilities, Future Prospects, and Governance* 88 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-and-governance.

[11] *Carpenter v. United States*, 585 U.S. 296 (2018).

[12] *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 348 (4th Cir. 2021) (*en banc*).

[13] https://mpctc.dpscs.maryland.gov/pdf/Body-Worn_Camera_Policy.pdf

required to follow,[14] generally bars "video or audio data from a body worn camera" from being "searched using facial or voice recognition software."[15]

The Maryland FRT policy should incorporate this existing requirement and should follow the lead of other jurisdictions in prohibiting use of FRT on both live and recorded video (including, but not limited to, video obtained from body-worn cameras). As the Detroit Police Department's policy puts it, "[m]embers [of the Department] 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."[16] Similarly, Massachusetts police are barred from using FRT on "moving images or video data."[17] These policies preserve the ability to extract a still frame from a video in order to use FRT to attempt to compare an image of a suspect against a matching database, while preventing FRT scanning of video to conduct automated tracking or identification of individuals' movements, activities, or associations over time.

III. Prohibit use of private FRT matching databases containing illegally collected faceprints

Senate Bill 182 addresses the types of matching databases that Maryland police can use when conducting FRT searches. The law authorizes use of (1) the state driver's license and identification card database, and (2) law enforcement mugshot databases. Md. Code, Crim. Proc. § 2-503(a)(2)(i). The law additionally permits use of a different matching database only if "[t]he law enforcement agency conducting the investigation has entered into an agreement with the entity that maintains the database governing the methods by which images in the database are collected." *Id.* § 2-503(a)(2)(ii). The Maryland FRT policy should provide guidance on the requirements of such agreements, to avoid facilitating violations of Maryland residents' rights.

Most FRT vendors provide algorithms that allow law enforcement agencies to conduct FRT searches against image databases supplied by the agency, typically either driver's license photos or mugshots. But at least one company in the U.S., Clearview AI, is marketing access to a very different, and more troubling, FRT database. Clearview has scraped more than 50 billion photos containing people's faces from the internet (including from social media accounts), and has extracted people's unique biometric identifiers from those photos without providing notice

---

[14] *See* Md. Code., Cts. & Jud. Proc. § 10-402(c)(11)(ii)(2); Pub Safety §§ 3-511(c) & (d).

[15] Maryland Police Training and Standard's Commission, Body-worn Camera Policy § I.2.b, https://mpctc.dpscs.maryland.gov/pdf/Body-Worn_Camera_Policy.pdf.

[16] Detroit Police Dep't, Directive No. 307.5 (Facial Recognition), § 3.2.

[17] Mass. Gen. Laws. Ann. ch. 6, § 220(a).

or obtaining consent. The company has been repeatedly sued over this practice under state biometric privacy and consumer protection laws.[18] Because of concerns with Clearview's abusive and extremely privacy-invasive collection of faceprints to populate its database, as well as the company's lack of transparency, law enforcement agencies in jurisdictions such as New Jersey and Los Angeles have prohibited their members from using Clearview.[19]

Clearview's practices violate the Maryland Online Data Privacy Act of 2024.[20] The law prohibits regulated companies from "collect[ing], process[ing], or shar[ing]" Maryland resident's biometric data (including faceprints used for facial recognition searches) unless "the collection or processing is strictly necessary to provide or maintain a specific product or service requested by" the individual to whom the biometric data pertains.[21] Clearview provides no product or service to the millions of Maryland residents whose biometric data it collects without consent; rather, it sells access to a facial recognition system that runs searches against that biometric data.

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND

The Maryland FRT policy should ensure that Maryland law enforcement agencies are not buying a product created in violation of Maryland residents' legal rights. The policy should require that any agreement for use of a third-party matching database must provide that neither the images in the database, nor the biometric identifiers (i.e. faceprints) extracted from those images, have been collected in violation of federal or state law or without consent. For maximum clarity, the policy should specifically prohibit use of Clearview AI by Maryland law enforcement.

* * * * *

---

[18] *See, e.g.*, Ryan Mac & Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database*, N.Y. Times (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html; Sara Merken, *Clearview AI Strikes 'Unique' Deal to End Privacy Class Action*, Reuters (June 13, 2024), https://www.reuters.com/legal/litigation/clearview-ai-strikes-unique-deal-end-privacy-class-action-2024-06-13/.

[19] Kashmir Hill, *New Jersey Bars Police From Using Clearview Facial Recognition App*, N.Y. Times (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html; Libor Jany, *Police Commission Sets New Rules for How LAPD Uses Surveillance Technology*, L.A. Times (Aug. 17, 2022), https://www.latimes.com/california/story/2022-08-17/lapd-adopts-new-rules-for-obtaining-using-t.

[20] Maryland Online Data Privacy Act of 2024, H.B. 567, 2024 Md. Laws Ch. 454, https://mgaleg.maryland.gov/2024RS/Chapters_noln/CH_454_hb0567e.pdf.

[21] Md. Code, Comm. Law § 14-4607(a)(1).

We appreciate your attention to this important issue. If you have any questions, or wish to discuss our views, please contact Yanet Amanuel at amanuel@aclu-md.org or (667) 219-2585.

Sincerely,

Nathan Fred Wessler
Deputy Director
ACLU Speech, Privacy, and Technology Project

Yanet Amanuel
ACLU-MD Public Policy Director

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

ROBERT JULIAN-BORCHAK WILLIAMS,

Plaintiff,

v.

CITY OF DETROIT, a municipal corporation, DETROIT POLICE CHIEF JAMES WHITE, in his official capacity, and DETECTIVE DONALD BUSSA, in his individual capacity,

Defendants.
_____/

Case No. 21-10827

Hon. Laurie J. Michelson
Mag. Judge David R. Grand

STIPULATED ORDER OF VOLUNTARY DISMISSAL WITH PREJUDICE

The parties, through their respective counsel, hereby stipulate and agree as follows:

1. Plaintiff and Defendants have reached a negotiated resolution in this matter. To that end, the parties have entered into a Settlement Agreement. *See* Exhibit 1 and the attachments thereto.
2. Pursuant to the stipulation of the parties and Fed. R. Civ. P. 41(a), and consistent with the above, all of Plaintiff's claims in this lawsuit against all Defendants are dismissed with prejudice and without costs.

3. The Court hereby retains jurisdiction to enforce the Settlement Agreement for four years from the date of the entry of this order.

IT IS SO ORDERED.

Dated: June 28, 2024

s/Laurie J. Michelson
LAURIE J. MICHELSON
UNITED STATES DISTRICT JUDGE

The parties stipulate to the entry of the above order:

/s/Michael J. Steinberg
Michael J. Steinberg (P43085)
Julia Kahn*
Nethra Raman*
Collin Christner*
Ewurama Appiagyei-Dankah*
Civil Rights Litigation Initiative
University of Michigan Law School
701 S. State St., Suite 2020
Ann Arbor, MI 48109
(734) 763-1983
mjsteinb@umich.edu
jekahn@umich.edu
nethra@umich.edu
collindc@umich.edu
eadankah@umich.edu

Philip Mayor (P81691)
Daniel S. Korobkin (P72842)
Ramis J. Wadood (P85791)
American Civil Liberties Union Fund of Michigan
2966 Woodward Ave.
Detroit, MI 48201
(313) 578-6803
pmayor@aclumich.org
dkorobkin@aclumich.org
rwadood@aclumich.org

Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
(212) 549-2500
nwessler@aclu.org

Counsel for Plaintiff

*Student Attorney practicing pursuant to Local Rule 83.21

/s/ Patrick M. Cunningham
Patrick M. Cunningham (P67643)
City of Detroit Law Department
2 Woodward Avenue, Suite 500
Detroit, MI 48226
(313) 237-5032
cunninghamp@detroitmi.gov

Counsel for Defendants

Dated: 6/25/24

EXHIBIT 1

Settlement Agreement with Attachments A-E

SETTLEMENT AGREEMENT
***WILLIAMS v. CITY OF DETROIT, et al.*,**
EASTERN DISTRICT OF MICHIGAN CASE NUMBER: 21-cv-10827

1. Preamble. The City of Detroit and Chief James White ("Defendants") recognize the need to safeguard the Fourth Amendment rights of individuals involved in a criminal investigation and to ensure that policy advances to keep pace with evolving technology used to fight crime in the City of Detroit, and therefore hereby enter into this settlement agreement with Plaintiff Robert Julian-Borchak Williams ("Plaintiff").

2. Purpose. Defendants and Plaintiff (collectively the "Parties") intend for this Agreement to settle and resolve the dispute referenced above, *Williams v. City of Detroit, et al.*, case number 21-cv-10827, filed in the United States District Court for the Eastern District of Michigan ("the Court"). This Agreement represents the compromise of a disputed claim and is not to be construed as an admission of liability on the part of Defendants.

3. Facial Recognition Manual Directive. Defendants agree to implement and enforce the attached Detroit Police Department ("DPD") Manual Directive 307.5 ("Facial Recognition"), which was approved by the Detroit Board of Police Commissioners (the "BOPC") on May 30, 2024. *See Attachment A*.

4. Facial Recognition Forms. Defendants agree to implement and instruct DPD personnel to use the attached investigative lead report and vetting

report forms. *See Attachment B*. DPD policy shall require that the relevant portions of these forms be completed by DPD Crime Intelligence Unit examiners and DPD investigators in connection with any facial recognition search.

5. Eyewitness Identification and Lineup Manual Directive. Defendants agree to implement and enforce the provisions of the attached DPD Manual Directive 203.11 ("Eyewitness Identification and Lineups") that have been added or changed between the date this lawsuit was filed on April 13, 2021, and the effective date of this Agreement, which was approved by the BOPC on May 30, 2024. *See Attachment C*.

6. Audit of Prior Cases. Within 180 days of the execution of this agreement, the DPD's Civil Rights Division will conduct an audit of all cases in which facial recognition technology was utilized to generate an investigative lead that was followed by an arrest or the issuance of an arrest warrant. The audit will be based upon a log of facial recognition requests maintained by DPD's Crime Intelligence Unit beginning on February 22, 2017. The audit will examine qualifying arrests made and arrest warrants issued through August 10, 2023. Auditors will identify all cases in which an arrest was made or a warrant was issued after an investigative lead was generated, and then determine: whether a live or photo lineup was utilized; whether there was an independent basis for the arrest such as an outstanding warrant or probable cause that the individual committed a

separate arrestable offense at another time or place; whether there was independent evidence supporting the arrest or issuance of the arrest warrant, and identify such independent supporting evidence in a written audit log. In the event that the audit reveals arrests made or arrest warrants issued following an investigative lead alone or an investigative lead and lineup identification that are unsupported by independent evidence, the DPD will notify the appropriate prosecutor. Active investigations subject to this audit shall comply with Manual Directives 203.11 and 307.5 prior to an arrest or the issuance of an arrest warrant.

7. Training Program. Defendants agree that DPD shall implement and abide by the attached Training Program for DPD for four years from the effective date of this agreement. *See Attachment D*.

8. Future Modifications to Manual Directives. Defendants may seek approval of future modifications of DPD Manual Directives 307.5 or 203.11 from the BOPC. However, Defendants agree that for four years following the effective date of this agreement, they shall not propose or make any substantive modifications that reduce, decrease, or remove protections in either policy that were added or changed between the filing of this lawsuit on April 13, 2021, and the effective date of this Agreement. This limitation on substantive modifications includes, but is not limited to any potential modification that would, (1) authorize investigators to conduct a lineup based on a facial recognition investigative lead

without first developing an independent and reliable basis for conducting the lineup, or to request an arrest warrant based only upon such a lineup combined with a facial recognition-derived investigative lead; (2) eliminate or reduce the number of supervisory officers who must approve investigative actions or arrest warrant requests made pursuant to either policy; (3) authorize photographic lineups to be conducted, (a) with a non-eyewitness, (b) in a non-blind fashion, (c) in a non-consecutive manner, or (d) containing a photograph derived from a facial recognition technology search; or (4) authorize DPD members to inform a witness to be administered a photographic lineup that facial recognition has been used to generate an investigative lead. When proposing any modifications of either policy to the BOPC, Defendants shall provide the proposed modifications to the ACLU Fund of Michigan.

9. Release of Claims for Damages, Attorneys' Fees, and Costs. The Parties agree that Plaintiff's claims for damages, attorney fees, and costs have been resolved as described in the attached General Release. See *Attachment E*. The Parties agree that Attachment E will be redacted in its entirety when this Agreement is filed with the court.

10. Breach of Terms. A breach of any term of this Agreement may be enforced by any party by filing a motion before the Court for enforcement of the Agreement. The party establishing a breach of this Agreement may be entitled to

equitable relief, costs, or attorney fees authorized by law, as determined by the Court.

11. Entry of Stipulated Order of Dismissal. Contemporaneous with the Parties' execution of this Agreement, the Parties through their counsel stipulate to the entry of an order of dismissal with prejudice ("Stipulated Order"), attached to which as an exhibit shall be an executed copy of this Agreement. The Stipulated Order shall expressly retain the Court's jurisdiction to enforce this Agreement for four years following the date of the Stipulated Order. In the event that the Court refuses to enter the Stipulated Order or retain jurisdiction to enforce this Agreement, this Agreement shall be null and void unless the Parties are able to agree to alternative terms.

12. Effective Date. This Agreement shall become effective immediately upon the Court entering the Stipulated Order.

13. Execution. This Agreement may be executed in counterparts, and is fully executed on the date by which both Parties have executed this agreement. Facsimiles and PDF versions of signatures will constitute acceptable, binding signatures for purposes of this Agreement.

14. Severability. If any provision of this Agreement, or part thereof, is held invalid, void, or voidable as against public policy or otherwise, the invalidity shall not affect other provisions, or parts thereof, which may be given effect

without the invalid provision or part. To this extent, the provisions, and parts thereof, of this Agreement are declared to be severable.

15. Entire Agreement. This Agreement and the attachments thereto contain all the terms and conditions agreed upon by and between the Parties. Other than the attachments to this Agreement, no oral agreement between Plaintiff and Defendants entered into at any time, nor any written agreement between Plaintiff and Defendants entered into prior to the execution of this Agreement regarding the subject matter of the instant proceeding, shall be deemed to have any force or effect, or to bind the Parties hereto, or to vary the terms and conditions contained herein.

Conrad L. Mallett, Jr. (P30806)
Corporation Counsel
City of Detroit Law Department

Date: June 24, 2024

Patrick M. Cunningham (P67643)
Attorney for Defendants
City of Detroit Law Department

Date: June 24, 2024

Michael J. Steinberg (P43085)
Julia Kahn*
Nethra Raman*
Collin Christner*
Ewurama Appiagyei-Dankah*
Civil Rights Litigation Initiative

Date: June 25, 2024

University of Michigan Law School
701 S. State St., Suite 2020
Ann Arbor, MI 48109
(734) 763-1983
mjsteinb@umich.edu
jekahn@umich.edu
nethra@umich.edu
collindc@umich.edu
eadankah@umich.edu

Philip Mayor (P81691)
Daniel S. Korobkin (P72842)
Ramis J. Wadood (P85791)
ACLU Fund of Michigan
Attorneys for Plaintiff
2966 Woodward Ave.
Detroit, MI 48201
(313) 578-6803
pmayor@aclumich.org
dkorobkin@aclumich.org
rwadood@aclumich.org

Nathan Freed Wessler
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, New York 10004
(212) 549-2500
nwessler@aclu.org

*Student Attorney practicing pursuant to Local Rule 83.21

Attachment A

Revised Manual Directive 307.5

Regarding Facial Recognition

Series 300 Support Services	Effective Date	Review Date Annually	Directive Number 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 *of Facial Recognition technology by* the Detroit Police Department (DPD). Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active or ongoing *investigation of a* Part 1 Violent Crime or a first-degree Home Invasion. If *an investigative lead* is *developed* through DPD's *F*acial *R*ecognition *program*, it shall be considered *only* an investigative lead *that shall not be the sole ground for arrest or to apply for an arrest warrant*.

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 *F*acial *R*ecognition data.

307.5 - 2.2 Examiner

An individual who has received advanced training in the *F*acial *R*ecognition *program* and its features. Examiners have at least a working knowledge of the limitations of *F*acial *R*ecognition. *Examiners are* qualified to assess image quality and appropriateness for *F*acial *R*ecognition searches and to perform one-to-many and one-to-one facial image comparisons.

307.5 - 2.3 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 - 2.4 *First-degree Home Invasion*
A person who breaks and enters a dwelling with intent to commit a felony, larceny, or assault in the dwelling, a person who enters a dwelling without permission with intent to commit a felony, larceny, or assault in the dwelling, or a person who breaks and enters a dwelling or enters a dwelling without permission and, at any time while he or she is entering, present in, or exiting the dwelling, commits a felony, larceny, or assault is guilty of home invasion in the first degree if at any time while the person is entering, present in, or exiting the dwelling either of the following circumstances exists:
(a) The person is armed with a dangerous weapon.
(b) Another person is lawfully present in the dwelling. (MCL 750.110a(2)).

307.5 - 2.5 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 - 2.6 *Predictive Analysis*
The process of using data to forecast future outcomes.

307.5 - 2.7 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 - 2.8 Statewide Network of Agency Photos (SNAP)
A computer application managed by the SNAP Unit, deployed through the 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 *F*acial *R*ecognition to surveil the public through any camera or video device.

307.5 - 3.2 Live Streaming or Recorded Videos
Members shall not use *F*acial *R*ecognition 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 *F*acial *R*ecognition.

307.5 - 3.4 Predictive Analysis
Members shall not use *F*acial *R*ecognition 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 *F*acial *R*ecognition 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*acial *R*ecognition to assess immigration status.

307.5 - 4 Discipline

1. Any violations to this policy shall be deemed major misconduct. Any misuse of the *F*acial *R*ecognition *program* will be investigated and reviewed for criminality. The remedy for this misconduct is dismissal from DPD.

2. If *F*acial *R*ecognition 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 *R*ecognition *technology* may only be used on a still image of an individual, *including still images captured from video.*

307.5 - 5.2 Criminal Investigation Required

Members shall not use *F*acial *R*ecognition technology unless *there is reasonable suspicion that use of Facial Recognition technology will provide information relevant to* an active or ongoing *investigation of a* Part 1 Violent Crime or a *first-degree* Home Invasion.

307.5 - 5.3 *An Arrest or Arrest Warrant Request Following Use of Facial Recognition Technology Must Be Supported by Additional Independent Reliable Evidence*

Probable cause must be established for an arrest or for an arrest warrant request must be established using legally authorized methods other than Facial Recognition. Examples of other investigative methods may include, but are not limited to cellular data analysis; eyewitness testimony, establishment of a timeline, DNA, etc. A request for an arrest warrant, or an arrest, shall not be made solely on the basis of an investigative lead developed through Facial Recognition technology in combination with a lineup identification. A request for an arrest warrant, or an arrest, must be supported by additional independent reliable evidence.

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.

   a. *Members requesting Facial Recognition services shall affirm that they have completed investigative Facial Recognition training;*

   b. *Members performing Facial Recognition services shall confirm that the requesting member has made the affirmation above.*

307.5 - 5.5 *Process for Performing Facial Recognition*

1. *Prior to the use of Facial Recognition, a CIU examiner shall complete the Real Time Crime Center – Facial Recognition Vetting form, which shall contain:*
   a. *The requestor's name, rank, and command;*
   b. *Confirmation that the requestor has affirmed that they have completed investigative Facial Recognition training;*
   c. *The crime being investigated (Part 1 Violent Crime or first-degree Home Invasion);*
   d. *The role the individual in the probe image is reasonably suspected to have played in the incident; and*
   e. *A description of the probe image quality.*

2. *CIU shall reject a request for Facial Recognition when:*
   a. *The request fails to identify the requestor's name, rank or command;*
   b. *The requestor fails to affirm that they have completed investigative Facial Recognition training;*
   c. *The crime being investigated is not a Part 1 Violent Crime or first-degree Home Invasion;*
   d. *There is not a reasonable suspicion that the individual in the probe image had a role in the commission of the crime; or*
   e. *The quality of the probe image is unsuitable for Facial Recognition.*

3. CIU shall perform Facial Recognition searches utilizing SNAP, which includes 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.

4. If the examiner *develops* an investigative lead, the examiner must corroborate this lead with at least one other examiner and a CIU supervisor. *Both examiners and the CIU supervisor shall sign off on the investigative lead.*

5. Upon final approval, CIU shall complete *an investigative lead* report for the requestor. *This investigative lead report must be attached to any request for a warrant for any person named in the investigative lead report.* The investigative lead report shall include the following language:

307.5 Facial Recognition

- "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 *independent* investigation and investigative resources."

- *"Facial Recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the probe image's quality, lighting, face angle, and face obstructions, among other factors."*

- *"Facial Recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).*

In addition, the investigative lead or vetting report shall also:

- *Disclose the probe image used to run the Facial Recognition search (in both its original form and with any enhancements), and identify all features of the probe image that may reduce the reliability of the Facial Recognition result (such as low light, low pixel density, angle of face, partial occlusion of face, etc.), and any enhancements or modifications made to the probe image during the course of the search process;*

- *Disclose each of the following: the date the investigative lead image was taken, how many other images of the same individual in the investigative lead image exist in the database that was searched, and, if other images of the same individual exist in the database, the dates when each was taken.*

6. *In any case in which charges are filed and in which Facial Recognition technology was used at any stage of the investigation, the member responsible for that investigation shall provide the following to the Wayne County Prosecutor's Office (WCPO):*

    - *Any investigative lead report and vetting report;*

7. In the event that *an investigative lead* cannot be developed, the requestor will be notified that no *investigative lead was developed*.

307.5- 5.6 Outside Agency Using Facial Recognition

An outside agency, or investigators from an outside agency, may request *Facial Recognition* searches *by DPD* 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 *DPD* 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 *independent* investigation and investigative resources."

c. If any agency is found not in compliance with this Directive, *DPD* 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 & *CIU* Responsibilities

1. The primary responsibility for the operation of *DPD*'s criminal justice information systems, *F*acial *R*ecognition 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 *F*acial *R*ecognition program to ensure compliance with applicable laws, regulations, standards, and policy;
   b. Acting as the authorizing official for individual access to *F*acial *R*ecognition 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 *CIU* will be responsible for the following:

   a. Reviewing *F*acial *R*ecognition search requests, reviewing the results of *F*acial *R*ecognition searches, and returning the most likely candidates – or candidate images – if any, to the requestor.
   b. Ensuring and documenting that personnel (including investigators from external agencies who request *F*acial *R*ecognition searches) meet all prerequisites stated in this policy prior to being authorized to use the *F*acial *R*ecognition system.

4. *Members of investigative entities shall be responsible for the following:*

   a. In the event that the Facial Recognition program develops an investigative lead, prior to making any probable cause arrest, or requesting a warrant from the (WCPO), the member must obtain written approval from their commanding officer and the commanding officer of Investigative Operations.

5. *DPD* 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 *DPD*'s *F*acial *R*ecognition information collection, receipt, access, use, dissemination, retention, and procedure.

307.5 - 6.2 Weekly 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 *F*acial *R*ecognition requests that were fulfilled, the crimes that the *F*acial *R*ecognition requests were attempting to solve, the number of leads developed from the *F*acial *R*ecognition *program, and the number of searches that did not produce investigative leads*. 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, *DPD* shall notify the Board of Police Commissioners.

307.5 – 6.3 Annual Report to the Board of Police Commissioners

DPD 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 *DPD*'s *F*acial *R*ecognition technology. The evaluation shall include any relevant lawsuits or settlements involving *F*acial *R*ecognition, the number of cases *in which* 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
DPD shall seek the Board of Police Commissioners' approval regarding any and all changes to *this manual directive*.

307.5 - 7 Security and Maintenance

1. *DPD* 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 *DPD* activity. *DPD*'s *F*acial *R*ecognition 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 *DPD*'s *F*acial *R*ecognition information from outside the facility will be allowed only over secure networks. All results produced by *DPD* as a result of a *F*acial *R*ecognition 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 *DPD*'s information or information systems will report a suspected or confirmed breach to their immediate supervisor who will ensure that the LASO) 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, *or* electric. Following assessment of the suspected or confirmed breach and as soon as practicable, *DPD* will notify the originating agency from which the entity received *F*acial *R*ecognition information of the nature and scope of a suspected or confirmed breach of such information. *DPD* will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

3. All *F*acial *R*ecognition equipment and *F*acial *R*ecognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.

4. *DPD* will store *F*acial *R*ecognition 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 *DPD*'s *F*acial *R*ecognition 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 *F*acial *R*ecognition system are not transferrable, must not be shared by *DPD* members, and must be kept confidential.

7. The system administrator (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 *DPD*'s *F*acial *R*ecognition 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. *DPD* will maintain an audit trail of requested, accessed, searched, or disseminated *F*acial *R*ecognition information. An audit trail will be kept for a minimum of one (1) year of requests, access, and searches of *F*acial *R*ecognition information for specific purposes and of what *F*acial *R*ecognition 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.

Attachment B

Investigative Lead Report and Vetting Report Forms

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 independent investigation and investigative resources.

Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors.

Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REAL TIME CRIME CENTER — FACIAL RECOGNITION INVESTIGATIVE LEAD

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 independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REQUEST #:	23-00				
REQUEST DATE/TIME:					
REPORT NUMBER:					
CRIME:	☐Homicide ☒Robbery/Carjacking ☐Aggravated Assault/NFS ☐CSC 1/CSC 3 ☐Home Invasion 1				
REQUESTER NAME:		**RANK:**	Choose an item	**COMMAND:**	
REASON:	☒ Reasonable Suspicion of a Part I Violent Crime or First-Degree Home Invasion ☐ Physical Incapacity/Mental Incapacity/At-Risk Person/Deceased Person (Homicide Only)				
IMAGES:	**ORIGINAL IMAGE**		**INQUIRY IMAGE**		**INVESTIGATIVE LEAD**
IMAGE SOURCE:	Choose an item.		Choose an item.	SNAP	**Date**
IMAGE ENHANCEMENTS:	Choose an item.		Choose an item.	None	
# OF IMAGES PRODUCED IN GALLERY:		**# OF LEAD IMAGES IN DATABASE:**		**DATES OF LEAD IMAGES:**	
NAME:					
ALIAS:					
DOB:					
DL/PID #:					
SID #:		**FBI #:**			
ADDRESS:					
SOCIAL MEDIA:					
INCARCERATION STATUS:	Choose an item.	**SOURCE:**	Choose an item.	**DATE:**	
INVESTIGATIVE LEAD PROCESS:	☒ Statewide Network of Agency Photos (SNAP) ☒ DataWorks Plus ☐ Forwarded to Michigan State Police (MSP) for additional assistance				
DATE/TIME FINALIZED:					
CIU PERSONNEL:					
CIU PEER REVIEWER:					
SUPERVISOR:					

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 independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

FURTHER INVESTIGATION WAS COMPLETED TO DETERMINE THE NECESSARY PROBABLE CAUSE TO PROCEED WITH AN ARREST OF THE INDIVIDUAL AND/OR SUBMISSION OF A WARRANT:

- ☐ CODIS Match
- ☐ AFIS hit
- ☐ CDR warrant results
- ☐ PEN warrant results
- ☐ Social Media warrant results
- ☐ Witness Statements
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____

INVESTIGATIVE OPERATIONS:

Prior to an arrest of an individual and/or submission of a warrant, the information was reviewed and:

- ☐ APPROVED
- ☐ DENIED

Investigate Operations Captain (print): _____

Signature: _____ **Date:** _____

COMMANDING OFFICER:

Prior to an arrest of an individual and/or submission of a warrant, the information was reviewed and:

- ☐ APPROVED
- ☐ DENIED

Commanding Officer (print): _____

Signature: _____ **Date:** _____

REAL TIME CRIME CENTER — FACIAL RECOGNITION VETTING

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 independent investigation and investigative resources. Facial recognition technology's accuracy depends in part on the ability to discern facial details. Thus, the accuracy of a facial recognition result depends on the input image's quality, lighting, face angle, and face obstructions, among other factors. Facial recognition error rates increase as the quality of the probe image decreases; however, even when using a high-quality probe image, facial recognition technology can still fail to provide an accurate result. Any result provided by the technology will always be false when the suspect does not have a photo in the comparison database (for example, no prior arrest photos in an arrest-photo database).

REQUEST DATE/TIME:					
REPORT NUMBER:					
CRIME:	☐Homicide ☐Robbery/Carjacking ☐Aggravated Assault/NFS ☒CSC 1/CSC 3 ☐Home Invasion 1				
REQUESTER NAME:		**RANK:**	Choose an item.	**COMMAND:**	
IMAGE SOURCE:			**NUMBER OF IMAGES:**		
REASON:	☒ Reasonable Suspicion of a Part I Violent Crime or First-Degree Home Invasion ☐ Physical Incapacity/Mental Incapacity/At-Risk Person/Deceased Person (Homicide Only)				

PER POLICE REPORT, SUPPLEMENTS, AND DETECTIVE NOTES:

PROBE ROLE IN CRIME:	Choose an item.
SUSPECT KNOWN:	Choose an item.

PHOTO QUALITY:

FILE SIZE:		**DIMENSIONS:**	
RACE:		**SEX:**	
FACIAL OBSTRUCTIONS:			
FACE ORIENTATION:			
IMAGE BRIGHTNESS:			
TATTOOS/FACIAL PIERCINGS/BIRTH MARKS:			
NUMBER OF USABLE IMAGES:			

STATUS OF REQUEST:	Choose an item
IF REJECTED, WHY?	

ANALYST:		**DATE/TIME:**	
REVIEWER:		**DATE/TIME:**	
SUPERVISOR:		**DATE/TIME:**	

Intel Number:	**23-**

Attachment C

Revised Manual Directive 203.11

Regarding Eyewitness Identification and Lineups

ral

DETROIT POLICE DEPARTMENT MANUAL

FSeries 200 Operations	Effective Date	Review Date *Two Years*	Directive Number **203.11**
Chapter 203 – Criminal Investigations			
Reviewing Office *Investigative Operations*			☐ New ☐ Directive ☒ Revised Revisions in *italics*
References			

EYEWITNESS IDENTIFICATION AND LINEUPS

203.11 - 1 PURPOSE

The purpose of this directive is to establish the guidelines for eyewitness identification *procedures involving showups, photo arrays, and live lineups. Erroneous eyewitness identifications have been cited as the factor most frequently associated with wrongful convictions. Therefore, in addition to eyewitness identification, all appropriate investigative steps and methods should be employed to uncover evidence that either supports or eliminates the suspect identification.*

203.11 - 2 POLICY

Members shall strictly adhere to this directive in order to maximize the reliability of identifications, minimize *erroneous identifications, and gather evidence that conforms to established legal procedures.*

203.11 - 3 Definitions

203.11 - 3.1 *Administrator*

The law enforcement official conducting the identification procedure.

203.11 - 3.2 *Double-Blind Presentation*

The administrator conducting the identification procedure does not know the suspect's identity.

203.11 - 3.3 *Filler*

A live person, or a photograph of a person, included in an identification procedure who is not considered a suspect.

203.11 - 3.4 *Live Lineup*

The process of presenting live individuals to an eyewitness for the purpose of identifying or eliminating suspects.

203.11 - 3.5 *Photo Array*
A means of presenting photographs to an eyewitness for the purpose of identifying or eliminating suspects.

203.11 - 3.6 *Sequential*
Presentation of a series of photographs or individuals to a witness and or a victim one at a time.

203.11 - 3.7 *Showup*
The presentation of a suspect to an eyewitness within a short time frame following the commission of a crime to eliminate them as a possible perpetrator. Showups, sometimes referred to as field identifications, are conducted in a contemporaneous time frame and proximity to the crime.

203.11 - 3.8 *Simultaneous*
Presentation of a series of photographs or individuals to a witness and or a victim all at once.

203.11 – 3.9 *Victim*
For purposes of this directive, an individual who is allegedly the victim of a crime and who also meets the definition of Witness under this policy.

203.11 – 3.10 *Witness*
For purposes of this directive, an eyewitness, meaning an individual who saw the suspect in person.

203.11 - 4 Procedures

203.11 - 4.1 *Showups*
The use of showups should be avoided whenever possible in preference to the use of a live lineup or photo array procedure. However, when circumstances require the prompt presentation of a suspect to a witness and or a victim, the following guidelines shall be followed to minimize potential suggestiveness and increase reliability:

a. *Document the witness's and or a victim's description of the perpetrator prior to conducting the showup. This description should be clearly noted as the witness and or victims' description and separate from the description noted by the member;*
b. *Conduct a showup only when the suspect is detained within a reasonable time frame after the commission of the offense and within a close physical proximity to the location of the crime;*
c. *Members shall obtain supervisory approval before conducting a showup;*

203.11 Eyewitness Identification and Lineups

d. Do not use a showup procedure if probable cause to arrest the suspect has already been established;
e. Transport the witness and or the victim to the location of the suspect whenever possible. Members shall not transport the suspect to the witness and or victim;
f. If possible, avoid conducting a showup when the suspect is in a patrol vehicle, handcuffed, or physically restrained by Department members, unless safety concerns make this impractical;
g. Do not take a suspect to the witness's and or victim's residence unless it is the scene of the crime and without the consent of both the suspect and the witness or victim;
h. Caution the witness and or victim that the person they are about to see may or may not be the perpetrator – and it is equally important to clear an innocent person. The witness and or victim should also be advised that the investigation will continue regardless of the outcome of the showup;
i. Do not conduct the showup with more than one witness and or victim present at a time;
j. Separate witnesses and or victims and do not allow communication between them before or after conducting a showup;
k. If one witness and or victim identifies the suspect, use a live lineup or photo array for remaining witnesses;
l. Do not present the same suspect to the same witness and or victim more than once;
m. Do not require showup suspects to put on clothing worn by, speak words uttered by, or perform other actions of the perpetrator;
n. Members should avoid words or conduct of any type that may suggest to the witness and or victim that the individual is or may be the perpetrator;
o. Remind the witness and or victim not to talk about the showup to other witnesses and or victims until police or prosecutors deem it permissible;
p. Videotape the identification process using an in-car or body-worn camera;
q. Members shall not use a cellular phone or other mobile communication device for a showup; and
r. Members shall document the time and location of the showup, the members present, the result of the procedure, and any other relevant information on their officer's daily report.

203.11 - 4.2 *Basic Procedures for Conducting a Live Lineup or Photo Array*

1. *A live lineup or photo array may only be administered to a witness and or victim as defined in this policy.*
2. *Prior to conducting a live lineup or photo array, members shall have the witness and or victim provide a recap of the incident to provide clarity that the witness and or victim has actual recollection of the incident and the suspect.*
3. *Prior to conducting a photographic line-up, a supervisor shall ensure that there is an independent basis supported by reliable evidence that the suspect, who will be presented in the line-up, committed the crime. An investigative lead generated by a search using facial recognition technology does not alone constitute an independent basis that the person selected as the lead committed the crime.*
4. *The photographic lineup shall not contain an image derived from facial recognition.*
5. *All photo lineups will be conducted using the sequential, double-blind presentation technique to ensure effective eye-witness identification. This means that an investigator, other than the lead investigator, who does not know who the suspect is, will present the line-up to the witness and or victim. It also means that photographs will be presented one-by-one to the witness and or victim.*
6. *The live lineup or photo array should consist of a minimum of six (6) individuals or photographs. Use a minimum of five (5) fillers and only one suspect.*
7. *Fillers should be reasonably similar in age, height, weight, and general appearance and be of the same sex and race, in accordance with the witness's and or victim's description of the offender.*
8. *Avoid the use of fillers who so closely resemble the suspect that a person familiar with the suspect might find it difficult to distinguish the suspect from the fillers (i.e., twins, look-alikes, facial recognition derived images, etc.).*
9. *Create a consistent appearance between the suspect and the fillers with respect to any unique or unusual features (e.g. scars, tattoos, facial hair) used to describe the perpetrator by artificially adding or concealing that feature on the fillers.*
10. *If there is more than one suspect, include only one in each live lineup or photo array.*
11. *During a double-blind presentation, no one who is aware of the suspect's identity should be present during the administration of the photo array. However, during a live lineup, the witnessing attorney should be present.*
12. *Place suspects in different positions in each live lineup or photo array.*
13. *Neither witnesses nor victims should be permitted to see or be shown any photos or images of the suspect prior to or during the live lineup or photo array other than the photo of the suspect included in the photo array at the time it is administered.*
14. *The live lineup or photo array should be shown to only one witness and or victim at a time; in order to prevent participating witnesses and or victims from being aware of the responses of other witnesses and or victims, members should separate witnesses and or victims and warn them not to communicate with each other about the lineup or images involved in the lineup until all witnesses and or victims have completed the live lineup or photo array.*

15. *Multiple identification procedures should not be conducted in which the same witness and or victim views the same suspect more than once.*
16. *Members shall not use statements, cues, casual comments, or provide unnecessary or irrelevant information that in any manner may influence the witnesses' and or victim's decision-making process or perception. In investigations where facial recognition technology was used prior to the lineup, members shall not inform the witness or victim that facial recognition technology was used or that it generated information contributing to the inclusion of an individual in the lineup.*
17. *The proceeding must be conducted in a fair manner, so as not to be unduly suggestive of the suspect. This is important because any remarks could later be interpreted as an attempt to influence the identification.*
18. *The administrator shall ask the witness and or victim to complete and sign a live lineup or photo array form at the time of the lineup. As part of the form, the witness and or victim shall record their degree of confidence in their identification.*
19. *Live lineup and photo array procedures shall be video and audio recorded, unless doing so is not possible. If a procedure is not recorded, a written record shall be created and the reason for not recording shall be documented. In the case of live lineups that cannot be recorded, members shall take and preserve a still photograph of each individual in the lineup.*
20. *The administrator shall document all parties present during the live lineup.*

203.11 - 4.3 *Photographic Arrays*

Prior to conducting a photographic lineup, a supervisor shall ensure that there is an independent basis supported by reliable evidence that the suspect, whose picture is to be presented in the course of the photo lineup, committed the crime. An investigative lead generated by a search using facial recognition technology does not alone constitute an independent basis.

1. *When creating a photo array, members shall follow the below guidelines:*
   a. *Do not use a facial recognition derived image;*
   b. *Use photos contemporary to when the crime occurred;*
   c. *Use black and white photos only if there are no color photos available;*
   d. *Do not mix color and black and white photos;*
   e. *Use photos of the same size and basic composition;*
   f. *Never mix mug shots with other photos;*
   g. *Do not include more than one photo of the same suspect; and*
   h. *Cover any portions of mug shots or other photos that provide identifying information on the subject – and similarly cover other photos used in the array.*
   i. *Do not use images of people who so closely resemble the suspect that a person familiar with the suspect might find it difficult to distinguish the suspect from the fillers (i.e., twins, look-alikes, facial recognition derived images, etc.).*

2. *The sequential procedure process should be preserved as part of the case file.*
3. A *witnessing* attorney *must* be present if a witness and or victim views photographs when the suspect is in custody. *Members shall obtain the attorney's information including their name, phone number, address, and state bar number.*
4. The attorney shall initial photocopies of all photographs used in the *photo array*. The officer in charge of the case shall ensure that attorneys witnessing the photo *array* are provided with a document outlining the attorney's role at the photo show up.
5. Where a witness and or victim identifies the suspect through the use of photographs, the "totality of the circumstances" test is used to determine whether the photographs utilized are not unnecessarily suggestive of any particular suspect.

203.11 - 4.4 *Live Lineups*

1. *When conducting the live lineup, members shall follow the below guidelines:*

   a. *The administrator of a live lineup must be a blind administrator who does not know the identity of the suspect;*
   b. *Ensure that all persons in the live lineup are numbered consecutively and are referred to only by number; and*
   c. *Document all parties present at the live lineup.*

2. *The officer in charge of the case is responsible for the following:*

   a. *Scheduling the live lineup on a date and at a time that is convenient for all concerned parties, to include the witnessing attorney and any witnesses and or victims;*
   b. *Ensuring compliance with any legal requirements for transfer of the subject to the live lineup location if they are incarcerated at a detention center; and*
   c. *Making arrangements to have persons act as fillers.*

3. A written record, the *Lineup* and Photo Identification Record (DPD355), should include:
   a. Names, *age,* and addresses of all persons whose photographs are to be used in the *live lineup or photo array*;
   b. Physical description of all persons whose photographs are to be used in the *live lineup or photo array*;
   c. Names and addresses of all persons present at the *live lineup or photo array*;
   d. Statements of identifying witnesses and or victims while making the identification; and
   e. *The witness's and or victim's degree of confidence in their identification, as specified above in 203.11 – 4.2(18).*

4. A *live* lineup cannot be avoided by having a witness and or victim view photographs when a formal *live* lineup is *reasonably* possible. *A photo array shall* not *be* conducte*d* if the suspect is in custody, unless:
   a. It is not possible to arrange a proper lineup;
   b. There are an insufficient number of persons available with the defendant's physical characteristics;
   c. The nature of the case requires immediate identification;
   d. The witnesses and or victims are *physically unable to attend a lineup*; or
   e. The subject refuses to participate in a lineup and by this action would seek to destroy the value of the identification.

5. All live lineups shall be photographed.
   a. The name, rank, and assignment of the *member* taking the photograph shall be entered on the *Lineup* and Photo Identification Record (DPD355), in the box designated "OTHERS PRESENT." The photograph shall then be attached to the *Lineup* and Photo Identification Record and become a permanent part of the court file.
   b. The officer in charge of the case shall be responsible for the photographing of lineups conducted at all other locations.

203.11 - 4.5 Refusal of Detainee to Stand in a Lineup

1. If a detainee refuses to stand in a lineup, the following procedures shall be followed:
   a. A determination shall be made as to the availability of a photograph of the detainee suitable for use in photograph identification; and
   b. Photograph identification can be used in lieu of a lineup if the subject refuses to participate in a lineup and, by the subject's action, would seek to destroy the value of the identification.

2. Regardless *of* whether a photograph is available or not, between the hours of 8:30 a.m. to 4:30 p.m. on weekdays and from 8:30 a.m. to 1:00 p.m., on Saturdays, Sundays, and holidays, the Wayne County Prosecutor's Office shall be contacted. *At any other time*, the Control Desk shall be contacted for the number of the on-duty assistant prosecuting attorney.
3. The prosecuting attorney contacted shall be informed if a photograph of the detainee is available or not and shall be informed that the detainee refuses to participate in a lineup. Department members and detention personnel shall be guided by the advice of the prosecuting attorney. Although the Michigan Supreme Court has ruled that forced participation in a lineup does not constitute unreasonable search and seizure, no force shall be exerted to force participation of a detainee in a lineup unless the prosecuting attorney contacted gives direction for such action.

203.11 - 4.6 *Limited Use of Video for Identification Purposes*

Members shall only utilize video to confirm the identity of a subject should the witness and or victim be a close associate or family member of the subject (e.g. mother / father or close friend).

203.11 - 5 Witnessing Attorney

1. *A witnessing attorney shall be present for all live lineups and photo arrays when the suspect is in custody.*
2. *Should the suspect be criminally charged and have obtained a lawyer, then the suspect's defense attorney shall act as a witnessing attorney. In all other cases, the officer in charge of the case shall call Notification and Control who shall identify the witnessing attorney.*
3. The purpose *of the witnessing attorney*'s presence is not to interfere with the conduct of the *live* lineup or *photo array* but to observe the procedures used by the law enforcement officers, so that in any subsequent court proceeding the accused will have a lawyer as a witness to any unfair suggestive procedures that may have been employed during the lineup or *photo array*.
4. Under no circumstances may a lawyer interfere with the conduct of the *live* lineup. While counsel may advise a client not to make incriminating statements, counsel may not advise a client to refuse to participate in the *live* lineup or any requested physical demonstrations *including a voice test, a handwriting sample, to wear certain clothing to assume a stance, to walk or to gesture*. If any lawyer should so advise a client, the Prosecuting Attorney's Office should be notified so that appropriate action may be considered.
5. *The OIC's responsibility is to document any objections, procedural violations, or other concerns voiced by the witnessing attorney during the live lineup or photo array.*

Attachment D

Training Provisions

Training Provisions for Settlement in *Williams v. City of Detroit*

1. The Detroit Police Department (DPD) will continue its current practice of requiring all newly promoted or newly hired detectives to complete a detective training school (currently known as the Detective Promotional Assessment Course (DPAC)). In addition to its current components, the detective training school shall include:
    a. A unit on the basics of how facial recognition technology functions, what features of a probe image can affect the reliability of the result of a facial recognition search, and why facial recognition technology alone should not be relied on for a positive identification;
    b. A unit on all of the requirements of DPD's manual directive on facial recognition;
    c. A unit on all of the requirements of DPD's manual directive on eyewitness identification and lineups.
2. DPD shall provide its sworn officers with training on the manual directives for facial recognition and for eyewitness identification and lineups as part of their annual in-service training. Training on both policies will also be incorporated into the training programs for new sergeants and lieutenants (SPAC and LPAC programs).
3. DPD shall train detectives, investigators, or supervisors of detectives and investigators stationed in each precinct detective unit (PDU) that utilize facial recognition technology on how facial recognition technology functions.
    a. The facial recognition training shall include training on the following subjects:
        i. That a facial recognition investigative lead is not a positive identification;
        ii. The basic steps that occur in a one-to-many facial recognition search, the image databases that are searched by each algorithm and what type of photos are contained in each database, the standards by which the system identifies possible matches, and the human process of morphological comparison that follows;
        iii. The fact that the accuracy of a facial recognition result depends on the probe image's quality, lighting, face angle, and face obstructions, among other factors;
        iv. The requirements of Manual Directive 307. 5-3, 307.5-4, 307.5-5.3, 307.5-5.4;
        v. Understanding the Investigative Lead Report and the Vetting Report.
        vi. The fact that studies have shown that facial recognition technology is not as accurate at identifying people with darker skin tones as it is at identifying white people.
    b. The facial recognition training shall be conducted by one or more trained facial recognition examiner(s) trained in the technical and operational details of the facial recognition system utilized by the Detroit Police Department and Michigan State Police.

c. DPD shall complete training under this section within one year of the date of this Agreement for all currently active detectives, investigators, or supervisors of detectives and investigators stationed in each precinct detective unit (PDU) that utilize facial recognition technology. This one-year timeline shall not include training of any sworn members who are unavailable for training due to an approved long-term leave of absence, including but not limited to members unavailable due to military service, disability, suspension, or family-emergency-medical-leave. Those members shall be trained as soon as practicable upon their return to active service with DPD.

Attachment E

General Release

GENERAL RELEASE

[redacted]