

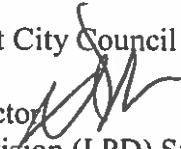
David Whitaker, Esq.
Director
Irvin Corley, Jr.
Executive Policy Manager
Marcell R. Todd, Jr.
Senior City Planner
Janese Chapman
Deputy Director

John Alexander
LaKisha Barclift, Esq.
M. Rory Bolger, Ph.D., AICP
Elizabeth Cabot, Esq.
Tasha Cowen
Richard Drumb
George Etheridge
Deborah Goldstein

City of Detroit
CITY COUNCIL
LEGISLATIVE POLICY DIVISION
208 Coleman A. Young Municipal Center
Detroit, Michigan 48226
Phone: (313) 224-4946 Fax: (313) 224-4336

Christopher Gulock, AICP
Derrick Headd
Marcel Hurt, Esq.
Kimani Jeffrey
Anne Marie Langan
Jamie Murphy
Carolyn Nelson
Kim Newby
Analine Powers, Ph.D.
Jennifer Reinhardt
Sabrina Shockley
Thomas Stephens, Esq.
David Teeter
Theresa Thomas
Kathryn Lynch Underwood
Wilson, Ashley

TO: The Honorable Detroit City Council

FROM: David Whitaker, Director 
Legislative Policy Division (LPD) Staff

DATE: September 6, 2019

RE: **Police Surveillance and Facial Recognition Technology**

On July 3, 2019, Council Member McCalister requested a comparative study of facial recognition technology and its use by the Detroit Police Department. This important and extremely contentious issue has been publicly discussed and received significant community and media attention several times, both in meetings of the Police Commission and the Public Health and Safety standing committee.

Even identifying an accurate and clear understanding of how facial recognition technology actually works is much more difficult than might be expected. The technology has multiple formats and is used for many other things besides law enforcement investigations. One scientific source generically describes the basic functions as follows: "Facial recognition is an advanced technology that helps in discerning and identifying human faces from an image or video. A system employed to perform facial recognition uses biometrics to map facial features from the photo or video. It compares this information with a large database of recorded faces to find a correct match." That source identifies the following steps in using this technology:

1. **Detection:** When the facial recognition system is attached to a video surveillance system, the recognition software scans the field of view of the camera for what it detects as faces. Upon the detection of each face-like image on a head-shaped form, it sends the face to the system to process it further. The system then estimates the head's position, orientation, and size. Generally, a face needs to be turned at least 35 degrees toward the camera for the camera to detect it.

2. **Normalization:** The image of the captured face is scaled and rotated so that it can be registered and mapped into an appropriate pose and size. This is called normalization. After normalization, the software reads the geometry of the face by determining key factors, include the distance between the eyes, the thickness of the lips, the distance between the chin and the forehead, and many others. Some advanced face recognition systems use hundreds of such factors. The result of this processing leads to the generation of what is called a facial signature.

3. **Representation:** After forming the facial signature, the system converts it into a unique code. This coding facilitates easier computational comparison of the newly acquired facial data to stored databases of previously recorded facial data.

4. **Matching:** This is the final stage in which newly acquired facial data is compared to the stored data; if it matches with one of the images in the database, the software returns the details of the matched face and notifies the end user.

There is a broad and deep controversy involving multiple privacy, criminal procedure, constitutional, technological and civil rights issues presented by this technology, which has included national and even international debates about the propriety and danger of using facial recognition technology, as well as police surveillance practices more generally. The Law Department's participation in framing and analyzing the legal principles would be very desirable, arguably even mandatory under the City Charter.

This preliminary report will begin by summarizing positions, both pro and con, regarding this technology. Recent local legislative bans and an Ohio state attorney general policy report on facial recognition technology are summarized and attached.¹ Key issues underlying the pro and con positions will be briefly listed and stated. Finally, the public positions taken by the Detroit Police Department and the Mayor regarding their current and anticipated use of facial recognition technology will be stated and evaluated, with an eye to clarifying the issues for future debates and policy development.

DPD's case for facial recognition technology

The Mayor and the Police Department stress the value of this technology as an investigative tool to counter violent crime. They deny that the City is using the technology for real time surveillance, or in connection with the Project Green Light security cameras. They cite actual instances where surveillance cameras have been used to apprehend suspects, distinguish this process from any use of facial recognition technology, and cite one successful use of facial recognition technology to identify an alleged criminal.

In essence, they depict facial recognition technology as merely a more efficient means of scanning a book of mug shots and identifying the similar appearing faces of potential wrongdoers based on the available photographic evidence and the technology's ability to rapidly biometrically identify similar-appearing individuals from a database of photographs. Crucially, they insist that merely linking a preexisting photo and an image from a crime scene generated by

¹ "Facial Recognition Inquiries; A Special Report" by Ohio Attorney General Dave Yost

the technology should not be enough to convict an individual, *i.e.*, it is not analogous to a DNA match.

The Mayor, in the attached detailed written policy message,² stresses that there have been no “negative incidents” in the two years that Detroit Police detectives have been using this technology. The Mayor’s official written statement further claims that “No one has proposed expanding its use.” However, multiple recent written orders from the Chief of Police (attached Manual Directives 307.6 from April 2019, and 307.5 from June 2019) indicate that the possibilities of using this technology for surveillance and sharing data with other security entities has been considered permissible to a significant extent.

The Mayor asks persuasively: “If your loved one was shot and there is a picture of the shooter, wouldn’t you expect the police to use every tool they can to identify the offender?” The Mayor now advocates a middle ground position, prohibiting use of facial recognition technology for surveillance, and permitting it for legitimate investigation. A proposed new formal written policy to that effect (attached, Manual Directive 307.5 from July 2019), together with a policy committee report, has been provided to the Board of Police Commissioners requesting their approval.

Critics’ case against facial recognition technology

Community and civil libertarian opponents of facial recognition technology argue that it violates human and constitutional rights of privacy and freedom of association. They point out that, whether or not the City itself is presently using such technology for real time surveillance, there are clear opportunities for quasi-private security agencies, of which there are several in greater downtown Detroit, to engage in such abuses; and it certainly would not prevent police officials using improved technical capacities from doing so in the future. In other jurisdictions to date, the use of this technology has been expanding very rapidly, with little to no meaningful regulation, so the possibility of current and future violations can hardly be ignored.

Federal law enforcement and immigration authorities are reportedly actively using this technology, posing an imminent and very serious threat to human rights, particularly under the current federal executive branch policies and administration. Of particular concern with this technology, even if it were limited to “merely” scanning mug shots more efficiently than human eyes, are a number of studies apparently demonstrating that the technology is particularly unreliable and inaccurate when applied to darker skin tones and perhaps other facial features of People of Color (and possibly also of women compared to men). Again crucially, opponents argue that the demonstrated unreliability of the technology, its inability to generate a conclusive “match” like DNA testing, gives police the opportunity to technologically justify what may amount to just another form of racial profiling; this concern has particular significance in a City with Detroit’s demographics.

Indeed, the creation of a technologically-derived group of suspects who never consented to their images being subjected to a technological selection investigative process triggers the constitutional privacy and criminal procedure protections of the Bill of Rights, endorses

² “Mayor Duggan: I Oppose of Facial Recognition Technology for Surveillance” July 18, see page 2 in particular

inherently unreliable investigative measures that raise the already-high risks of discrimination and false identification in criminal investigations, and even potentially expands the powers of police authorities to target vulnerable groups for intensified technological scrutiny.

Local bans on facial recognition technology

At least three cities, Oakland and San Francisco, California, and Somerville, Massachusetts, have already passed ordinances limiting the use of such technology. Their ordinances are attached. The Ohio Attorney General has also issued the attached written report prohibiting police in that state from using the technology without the state attorney general's approval.

The San Francisco ordinance is quite long and detailed. It seeks to regulate the use of "surveillance technology" rather than facial recognition technology *per se*, and relies heavily on transparency and formal reporting rather than a legislative ban. It states that "The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring." [P.2, paragraph (d)] But it appears to seek to strike a similar balance as the Mayor's most recent policy statement between legitimate investigative use of surveillance technologies generally, and their abusive use to target and oppress.

The Oakland ordinance, like the San Francisco law, emphasizes the historical record of using police surveillance to target vulnerable and disfavored groups. (P. 1, 2nd WHEREAS clause) Otherwise, it takes a similar approach to San Francisco's, without expressly denouncing the dangers of facial recognition technology "substantially outweigh[ing]" its "purported benefits", but arguably with some additional clarity and a clear ban on city officials using "surveillance technology", as opposed to facial recognition technology, without express approval of the local legislative body. There are many unresolved issues of applications of technology, standards for oversight, and how facial recognition technology itself relates to surveillance more generally. In LPD's judgment, neither Bay Area ordinance should be considered the last word on regulating this technology.

The Somerville ordinance simply bans use of facial recognition technology, and is much shorter than the Bay Area ordinances. Clearly one of the threshold determinations for City officials to make is whether to follow the Somerville policy of outright ban on facial recognition technology, or the Bay Area's favored approach of broad regulation of surveillance more generally.

The Ohio Attorney General issued a special report on facial recognition. It is attached. It relies on the state attorney general's office granting strictly controlled permission for law enforcement agencies to access databases for facial recognition technological exploitation, limiting it to legitimate criminal investigative purposes only.

Constitutional issues

The contentiousness of this debate arises out of at least three classic civil liberties issues: 1) How should the 18th century provisions of the Bill of Rights be applied to technological

investigative tools that the founders couldn't possibly have envisioned when they drafted our fundamental human rights law?³; 2) The oft-demonstrated reality that eyewitness perpetrator identification evidence is among the most inherently unreliable evidence known to courts of law⁴; and 3) The lack to date of effective regulation or limitation on potential abuses.

The Bill of Rights to the US Constitution, in addition to the First Amendment freedoms of speech and association, arguably threatened by selective application of this technology to disfavored groups, contains a basic set of criminal procedure provisions:

- The Fourth Amendment prohibition on unreasonable searches and seizures;
- The Fifth Amendment requirement of Due Process and prohibition on self-incrimination;
- The Sixth Amendment guarantee of speedy trial and rights to counsel and to call and confront witnesses;
- The Seventh Amendment guarantee of jury trial;
- The Eighth Amendment prohibition of cruel and unusual punishments; and
- The Fourteenth Amendment guarantees of Equal Protection and Due Process, applicable against the states and their local municipalities.

In light of the above bedrock protections for human liberty embedded in our fundamental law, it is hardly surprising that modern digital technologies seeking to enhance police abilities to identify and prosecute suspects based on impenetrable algorithmic processes, without any discernible regulatory oversight to date, raise the kinds of thorny issues discussed here. Rather, it would be frightening if residents of the City of Detroit did not care about these weighty concerns, particularly where the databases being searched include all State of Michigan

³ This factor alone explains why a complete study of this issue would take a long time (and would ideally be entrusted to a civil liberties expert scholar - or a team of them). To properly analyze facial recognition technology under the Bill of Rights would require detailed analysis and comparison of multiple prior US Supreme Court cases involving technologies that arguably invade privacy but didn't exist in the late 18th century when the Bill of Rights was adopted – wiretaps, infrared scanners, satellites, drones, sonograms, and other modern technologies used in “searches and seizures” of potential evidence of crimes. To summarize a vast and difficult analytical literature, there is no guarantee that technological advances necessarily enhance protection for human and civil rights and liberties. Quite the contrary, the framers of the Bill of Rights were revolutionaries. The suggestion that police officers' views of such issues in the 21st century are aligned with their intent is not warranted (pun intended).

⁴ This thorny criminal law issue of eyewitness identification highlights the flaw in any analogy between reliable scientific evidence like DNA testing and facial recognition technology, as a classic case of comparing apples to oranges. The potential for suggesting to a victim and/or witness that a computerized facial scan has fairly and reliably selected an individual as ‘looking like’ an alleged perpetrator should not be discounted as a major threat of unjust criminal prosecution and conviction. The claim that such a procedure is not as accurate or reliable as a DNA sample does not diminish the concern. On the contrary, it presents the above-mentioned serious concerns of technological bias confirmation, suggestion of a particular result, and racial discrimination, and on the basis of technology that the police admit is unreliable. The fact they are even making this argument that the technology is not like DNA evidence is very troubling, and suggests that the police (understandably in light of the scope and complexity of the relevant controversies) don't fully understand the seriousness of the issues and the profound concerns.

identification documents and driver licenses, subjecting virtually everyone in the state to nonconsensual searches.

The Police Department's argument that its facial recognition technology is a 'mere investigative tool', like the Mayor's argument that the Police Department under his supervision will not be abusing the technology, are ultimately unconvincing. In addition to documentary evidence that wider applications of the technology have already been ordered by the Police Department (Manual Directives 307.5 and 307.6), the potential for other public and private agencies to abuse this complex and secretive technology, and its potential to generate false convictions, cannot be discounted on these grounds. If these arguments are intended to support robust regulation of the technology, and its limitation to non-discriminatory automated searching of mugshots, as opposed to unfairly targeting the vulnerable and suggesting guilt based on inherently unreliable evidence and procedures, then it merely leads to continued controversy over what regulation of inherently unreliable tools is necessary and appropriate.

Moreover, the statement that in police officials' opinion a conviction should not be based on facial recognition technology identifying the defendant is not reassuring at all. That is a decision for a prosecutor, a jury and a trial judge with appellate judicial review in a particular case, not a basis for legislative policy making or police administration. In a hypothetical heinous criminal case, where an African-American defendant stands before an all-white tribunal (as occurs regularly in federal and suburban courts in and around Detroit), the claim that facial recognition technological identification would be insufficient to support a conviction flies in the face of virtually everything we know about race in the US criminal justice system and application of the Bill of Rights and other criminal procedures in racially charged contexts.


At a minimum, the administration's defense of current practices is an argument for better regulation, not against clear policy and regulation. Whether or not there should be such local legislative intervention, and whether it should take the form of restrictions on surveillance and oversight of investigation, as in Ohio and California, or an outright ban on facial recognition technology, as in Somerville, Massachusetts, are the issues for City Council in Detroit. The need for legislative oversight has been demonstrated. Its form should be the focus of the debate.

If Council has any other questions or concerns regarding this subject, LPD will be happy to provide further research and analysis upon request.

MEMORANDUM

TO: David Whitaker, Director
Legislative Policy Division Staff

THROUGH: Brenda Jones
President, Detroit City Council

FROM: Roy McCalister, Jr., Councilman 
City of Detroit

DATE: July 3, 2019

RE: **Legal Opinion(s) and/ or Comparative Study Regarding Facial Recognition Technology**

Mr. Whitaker:

I am interested in a comparative study as it pertains to the Facial Recognition Technology and its use by our Detroit Police Department as an investigative tool relative to crime investigations. I would like to know if you could research any applicable laws, pending legislation and/ or an unbiased analysis of the technology in use on the market today. Perhaps if there are any established legal opinions, practices, industry standards or suggested uses relating to the below listed questions?

1. Is the current technology any more invasive than the collection of finger prints or DNA samples?
2. How fast is the technology changing from day-to-day?
3. What legal parameters would you suggest be the minimal standard when using this technology?
4. Are there any Constitutional Rights infringements with the use of this technology when supplementing an investigation with the results of the facial recognition technological search and a possible identification of a potential suspect?
5. What if any safe guards do you recommend we employ to protect the City of Detroit in front of the use of the new technology?
6. Are there any current legal precedents anywhere in the United States relative to the new technology? (If so, please attach.)

Sincerely,



Roy McCalister, Jr.
Detroit City Council

CC:

Council President Brenda Jones
President Pro Tem Mary Sheffield
Council Member Janee' Ayers
Council Member Gabe Leland
Council Member Andre Spivey
Council Member James Tate
Council Member Scott Benson
Council Member Raquel Castaneda-Lopez
City Clerk

CITY CLERK 2019 JUL 3 PM 1:21

Legislative Policy

JUL 03 2019

MAYOR DUGGAN: I OPPOSE USE OF FACIAL RECOGNITION TECHNOLOGY FOR SURVEILLANCE

JULY 18

MAYOR'S OFFICE

Dear Residents of the City of Detroit:

There's been a lot of discussion and confusion the last couple weeks on the issue of the Detroit Police Department's use of facial recognition technology. Our residents too often suffer the pain and loss of violent crime. We expect the police to be vigorous in reducing that violence, but I wanted you to hear directly from me how I believe we need to balance that with the privacy rights of our community.

I strongly oppose the use of facial recognition technology for surveillance.

The Detroit Police Department does not and will not use facial recognition technology to track or follow people in the City of Detroit. Period. Detroiters should not ever have to worry that the camera they see at a gas station or a street corner is trying to find them or track them.

DPD is not permitted to use facial recognition software for surveillance and I will never support them doing so. The technology is just not reliable in identifying people from moving images and research has shown it is even less reliable in identifying people of color.

I have spoken to several members of the Detroit Police Commission and have encouraged them to continue this practice by formally adopting a "no surveillance" policy for facial recognition technology and providing for serious discipline for any DPD employee who violates this policy.

There have been a number of misleading reports that have confused Green Light or traffic cameras with facial recognition technology. They are not correct.

The Green Light cameras do not have any facial recognition technology – they are standard security cameras.

The traffic cameras we are proposing to purchase do not have any facial recognition technology – they are standard traffic cameras.

I fully support the use of cameras to address the violence in this community. I do not support the use of those cameras to conduct facial recognition surveillance.

Green Light cameras have been enormously successful without facial recognition

Nearly 600 businesses have voluntarily installed Green Light cameras in the last three years.

Carjackings in Detroit have dropped dramatically since Green Light started in 2016:

Total Carjackings Committed in Detroit

January – June 2015	222
January – June 2019	94 -58%

A 58% reduction in the number of carjacking victims is real progress. Detroiters constantly heard warnings not to stop for gas in the city at night. Today, you can see large numbers of customers at Green Light gas stations late every evening. They aren't perfect, but Green Light cameras have created zones of safety as prospective carjackers have learned that they are almost certain to be arrested and convicted when their crime is recorded on a high definition camera.

We Expect Traffic Cameras to be Successful in Reducing Drive-by Shootings without Facial Recognition

We have proposed cameras at major intersections to fill in the holes of the Green Light system to help identify vehicles used in shootings. This has nothing to do with facial recognition – that technology would be useless in identifying people in moving vehicles.

In January, a 3 year old boy was shot and killed on the Southfield Freeway on his way to Sesame Street Live. It was a case of random road rage normally very difficult for police to solve. But in this case, a gas station camera happened to catch a video of the silver Mercedes involved in the shooting as it exited the freeway and it was that video that led to the arrest of the shooter.

We continue to have far too many victims of drive-by shootings and far too many remain unsolved when police cannot conclusively identify the car. In the first week of July, we had 12 drive by shootings with 16 victims. 4 of them died. In each case we had a general description of the car from witnesses. For example:

Thursday, July 4th 9:55 PM: 61 Year Old Woman was shot on Orleans near Seven Mile by a shooter in a blue Chevy Malibu.

Friday, July 5th 1:46 AM: 25 Year Old Man was shot at Seven Mile and Conant by a shooter in a Burgundy Chevy Trailblazer

As of this morning, the police have not made arrests in either case. Had we had traffic cameras at major intersections, it is highly likely we would have license plate numbers and identifying characteristics of the Blue Malibu and Burgundy Trailblazer.

The gun violence in this city is completely unacceptable. Cameras at traffic intersections will help identify the vehicles of drive-by shooters and ultimately reduce the shootings. We do not need and will not use facial recognition surveillance on the traffic cameras to accomplish this.

The appropriate use of Facial Recognition Technology: learning the identity of dangerous offenders

The Detroit Police Department's purchase of facial recognition software was approved by Detroit City Council by a 6-0 vote in 2017. It has been used for the last two years by DPD detectives to identify dangerous offenders, without any negative incidents. No one has proposed expanding its use. Here's how it is used today:

Oftentimes police get a picture of an offender while committing a crime. It could come from a citizen's doorbell camera, a Green Light camera, or a private security camera. Often we ask for the public's help to identify the offender, showing their picture on the TV news.

Homicide detectives at times tried to identify an offender from a picture by spending hours looking through mug books. In the last two years, DPD has taken the picture of that unknown offender and used the facial recognition technology to try to find matching pictures in mug books and other records.

On November 25, at 5:49 AM at a (non-Green Light) gas station on Van Dyke, a 34 year old man was shot. The gas station's security camera got a clear picture of the shooter, but no one was able to identify him. A week later, the facial recognition software found a tentative match in a police mug book. Detectives pursued that lead and quickly found that the same suspect had posted a picture of himself on a public social media page wearing the identical distinctive jacket he had worn during the shooting. Subsequent police investigation positively confirmed his identity.

If your loved one was shot and there is a picture of the shooter, wouldn't you expect the police to use every tool they can to identify that offender? Police never make an arrest just because there is a facial recognition match. But it is an important source of leads detectives can use to find the identity of the offender. I fully support the technology's use for that limited purpose.

Summary

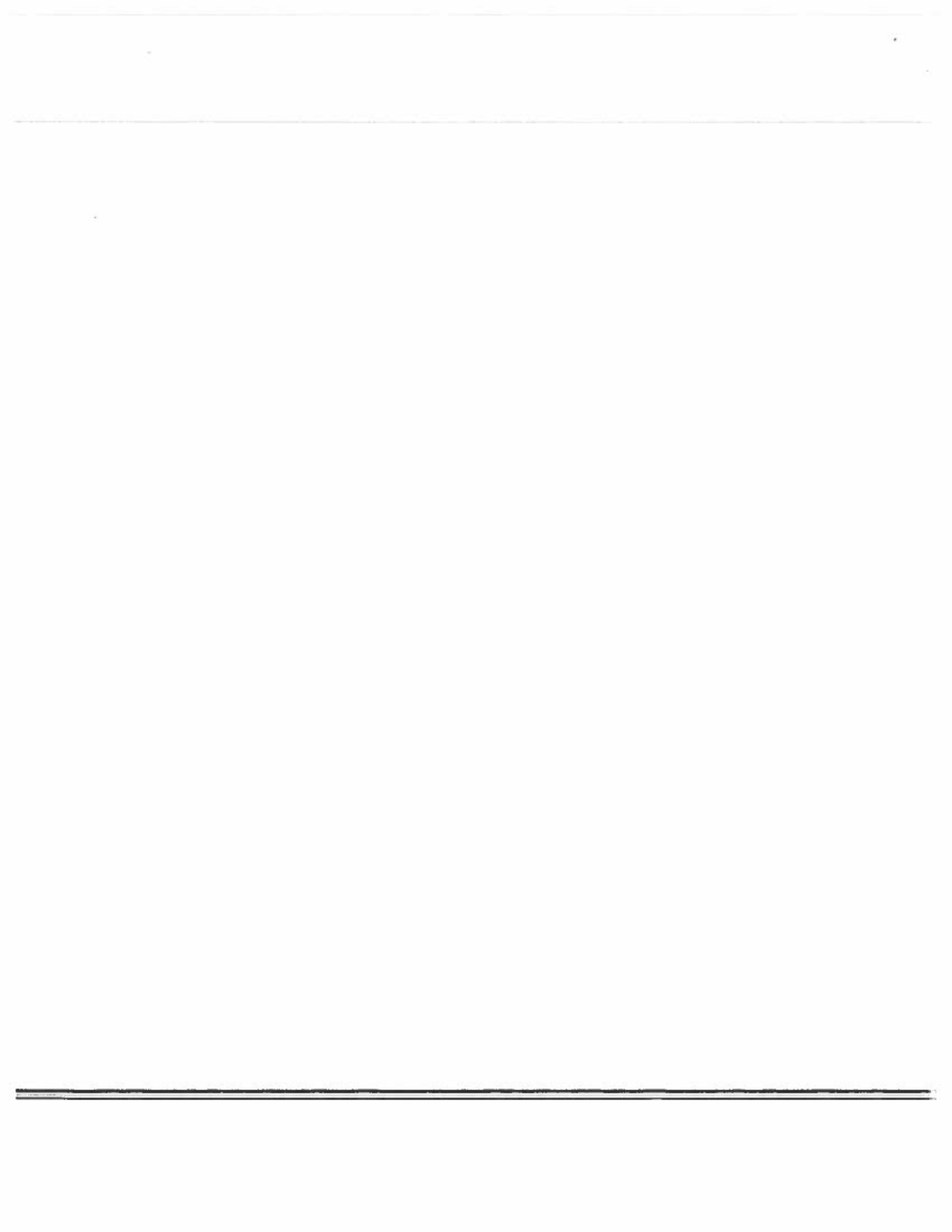
The Detroit Police Department has not and will not use facial recognition technology for surveillance. No one is watching you on any camera in this city with facial recognition software. I will not support the software ever being used in that way.

If you have committed a dangerous crime and the police have a picture of you, only then can police detectives use facial recognition software on that picture to try to determine your identity.

The most painful moments I experience as Mayor are conversations with the families of victims who just want to know when the police are going to make an arrest in the shooting. Those conversations are even more painful when the family knows the police have a picture of the offender and still can't make an ID. Facial recognition software can be very important in bringing peace to those families.

I hope the Board of Police Commissioners will adopt a policy that recognizes where this technology is helpful, but which also strictly prevents facial recognition surveillance and provides strong punishment for any abuse of that policy. It's my hope we can find common ground on this issue.

Michael E. Duggan
Mayor of Detroit



PLANNING, RESEARCH, AND DEPLOYMENT

TRANSMITTAL OF WRITTEN DIRECTIVE

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

TYPE OF DIRECTIVE: Manual Directive 307.6


SUBJECT: USE OF TRAFFIC LIGHT-MOUNTED CAMERAS AND FACIAL RECOGNITION TECHNOLOGY

ORIGINATED OR REQUESTED BY: Planning, Research, and Deployment

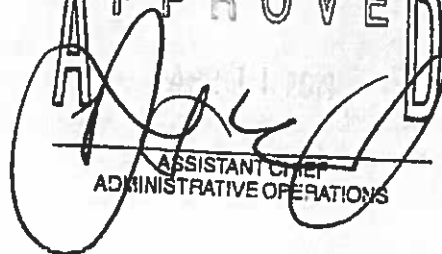
APPROVALS OR COMMENTS:

The above referenced directive is an updated directive. The information for this directive came from the Mayor's office (documentation included)

- Updated "Immigration Uses Prohibited" Section

A P P R O V E D
APR 22 2019

SECOND DEPUTY CHIEF
POLICE LEGAL ADVISOR

R E C E I V E D
APR 23 2019
BOARD OF POLICE COMMISSIONERS

A P P R O V E D

ASSISTANT CHIEF
ADMINISTRATIVE OPERATIONS

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

4711



Series 300 Support Services	Effective Date	Review Date Annually	Directive Number 307.6
Chapter 307 – Information System			<input checked="" type="checkbox"/> New Directive <input type="checkbox"/> Revised
Reviewing Office Office of Support Operations			
References:			

USE OF TRAFFIC LIGHT-MOUNTED CAMERAS AND FACIAL RECOGNITION TECHNOLOGY

307.6 - 1 PURPOSE

The purpose of this policy is to ensure that images and video footage from cameras that are mounted on traffic signals, or on Public Lighting Authority (PLA) poles (1) are used in a manner that honors the privacy of Detroit residents, while (2) providing Detroit Police Department (DPD) members the resources they need to ensure that Detroit neighborhoods are safe. The cameras subject to this policy, which include both PLA-pole mounted cameras and traffic-signal mounted cameras, are hereinafter referred to as "traffic light-mounted cameras."

307.6 - 1.1 Compliance with Applicable Laws

Any use of images and/or video footage from traffic light-mounted cameras is subject to applicable local, state, and federal law; including, but not limited to, the protections provided in the First, Fourth, and Fourteenth Amendments to the United States Constitution. This policy is subject to all applicable law. This policy is meant to provide additional protections beyond those already provided by law.

307.6 - 1.2 Relationship to other Department Policies

This policy provides requirements that are applicable to traffic light-mounted cameras only. It does not supersede any generally applicable Department policies with respect to other records or operating procedures. If this policy directly speaks to a subject that is also covered in a separate policy, this policy governs with respect to traffic light-mounted cameras only. If this policy is silent on a subject that is covered in a separate policy, the separate policy governs.

307.6 - 1.3 Discipline

Any violations to this policy specific to privacy, violation of use and private use shall be deemed egregious conduct.

307.6 - 1.4 Severability

If any term or section of this policy is found to be to any extent illegal, otherwise invalid, or incapable of being enforced, such term or section shall be excluded to the

DETROIT POLICE DEPARTMENT

MANUAL

307.6 Use of Traffic Light Mounted Cameras and Facial Recognition Technology

extent of such invalidity or unenforceability; all other terms or sections hereof shall remain in full force and effect.

307.6 - 2 Permissible Uses of Traffic Light-Mounted Cameras

Members may use footage and images obtained from traffic light-mounted cameras for legitimate law enforcement purposes only. For purposes of this policy, "legitimate law enforcement purposes" includes investigations into criminal activity; pursuit of a criminal suspect; monitoring an ongoing situation in which criminal activity is, or is reasonably expected to occur; and/or monitoring cameras at the Detroit Real-Time Crime Center (RTCC), where all generally applicable RTCC policies apply. The Crime Intelligence Unit must establish reasonable suspicion of criminal activity before creating or analyzing intelligence in any way gathered from traffic light-mounted cameras.

307.6 - 2.1 Traffic Enforcement and Related Monitoring Prohibited

Members are strictly prohibited from using footage or images obtained from traffic light-mounted cameras to enforce non-criminal traffic or pedestrian laws (e.g. red-light violations, jaywalking), or to issue civil infractions of any kind.

307.6 - 2.2 Immigration Uses Prohibited

DPD members are strictly prohibited from using footage or images obtained from traffic light-mounted cameras to assess immigration status or engage in immigration enforcement.

307.6 - 3 Placement of Cameras

Traffic light-mounted cameras will be positioned so that they provide video and images from public spaces only.

307.6 - 3.1 Accidental Capture of Private Spaces

If, notwithstanding the positioning of traffic light-mounted cameras as stated above, a traffic light-mounted camera accidentally captures video or images from a private area not accessible to the general public—including, but not limited to, a view of the interior of any building that is not visible from the street—members will not monitor that camera until it is repositioned to capture video and images from public spaces only.

307.6 - 4 Record Retention

307.6 - 4.1 Retention of Imagery

Subject to the exception listed in the below section (Evidence of Criminality), any video or images from a traffic light-mounted camera may be retained for no more than 30 days, and must be deleted and destroyed no later than 30 days after recording.

307.6 Use of Traffic Light Mounted Cameras and Facial Recognition Technology

The Department may, in its discretion, opt to retain video or images from a traffic light-mounted camera for fewer than 30 days.

307.6 - 4.2 Preservation of Evidence

Any recording that contains evidence of a criminal activity will be retained until the case is solved, closed, and litigation ends. Any recording that is subject to a lawful request to preserve evidence in a civil matter will be retained until that request is lifted or expires.

307.6 - 5 Use of Facial Recognition Technology**307.6 - 5.1 Criminal Investigation Required**

Members will not use facial recognition technology unless that technology is in support of an active or ongoing criminal or homeland security investigation.

307.6 - 5.2 Individualized Targeting

Members may 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 criminal or homeland security investigation.

**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 and Deployment

APPROVALS OR COMMENTS:

The above referenced directive is an updated to reflect the Board of Police Commissioners recommendations. Please see the Board's official recommendations also attached in this document.

A P P R O V E D
JUN 21 2019
[Signature]
SECOND DEPUTY CHIEF
POLICE LEGAL ADVISOR

Approved
[Signature]

A P P R O V E D
JUN 25 2019
[Signature]
ASSISTANT CHIEF
ADMINISTRATIVE OPERATIONS

R E C E I V E D
JUN 27 2019
BOARD OF POLICE COMMISSIONERS
11:45 PM 22nd, 2019

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

4262



DETROIT POLICE DEPARTMENT

MANUAL

Series 300 Support Services	Effective Date	Review Date Annually	Directive Number 307.5
Chapter 307 – Information System			
Reviewing Office Crime Intelligence			<input checked="" type="checkbox"/> New Directive <input type="checkbox"/> Revised
References:			

FACIAL RECOGNITION

307.5 - 1 PURPOSE

The purpose of this policy is to establish procedures for acceptable use of the images, information, and tools within the Detroit Police Department's (DPD) facial recognition software and the Statewide Network of Agency Photos (SNAP) application.

307.5 - 2 SYNOPSIS

1. A member has reasonable suspicion that an individual was involved in a Part 1 Violent Crime (robbery, sexual assault, homicide, or aggravated assault) or home invasion. The member obtains an image of this individual from a video fed into the Real Time Crime Center or another source.
2. Those still images are used to search known databases or repositories of criminal mugshots, state driver's license photographs, state identification card photographs, and sex offender registry photographs; (307.5-6 (1) and (2))
3. Images taken during a First Amendment-protected public event, activity, or affiliation will be utilized only for exigent circumstances which will require the signature of the Chief or designee and a report to the Board of Police Commissioners after such use (307.5-6(6) and (7)); and
4. DPD shall not use live streaming videos with the facial recognition software. (307.5-3(3))

307.5 - 3 POLICY

1. This policy was established to ensure that all images are lawfully obtained, including facial recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the Department. This policy also applies to the following:
 - a. Images contained in a known identity face image repository and its related identifying information;
 - b. The face image searching process;

DETROIT POLICE DEPARTMENT

MANUAL

307.5 Facial Recognition

- c. Any results from facial recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the Department; and
 - d. Lawfully obtained probe images of unknown suspects that have been added to unsolved image files, pursuant to authorized criminal investigations.
2. Authorized Department members, personnel providing information technology services to the Department, private contractors, and other authorized users will comply with the Detroit Police Department's Facial Recognition Policy and will be required to complete training that is mandated through the Department's Crime Intelligence Unit. In addition, authorized Department members tasked with processing facial recognition requests and submissions must also complete specialized training mandated through the Department's Crime Intelligence Unit. 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. The Detroit Police Department will provide a printed or electronic copy of this facial recognition policy to the following:
 - Department members who provide facial recognition services;
 - Participating agencies; and
 - Individual authorized users.
 - d. All technology associated with facial recognition, including all related hardware and software support, is bound by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy, particularly Policy Area 13, and the Michigan CJIS Security Addendum;
 - e. The information within the facial recognition databases is considered highly restricted personal information and personally identifiable information (PII) which

307.5 Facial Recognition

may only be transmitted, accessed, used, disseminated, and disposed of in accordance with state and federal laws, rules, policies, and regulations; including, but not limited to, the most recent federal CJIS Security Policy, the Michigan CJIS Security Addendum, the CJIS Policy Council Act (1974 PA 163), MCL 28.211-28.216, and the most current CJIS Administrative Rules; and

- f. Improper access, use, or dissemination of highly restricted personal information or PII obtained from the use of the Statewide Network of Agency Photos (SNAP) may result in criminal penalties and/or administrative sanctions. Criminal violations include, but are not limited to, those found in MCL 28.214 and MCL 257.903.

3. DPD shall not use live streaming videos with the Facial Recognition software.

307.5 - 4 Definitions**307.5 - 4.1 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 - 4.2 DataWorksPlus

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

307.5 - 4.3 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.

307.5 - 4.4 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 - 4.5 Highly Restricted Personal Information

An individual's photograph or image, social security number, digitized signature, medical and disability information.

307.5 - 4.6 Participating Agencies

Any outside agency authorized to request information from the Department's facial recognition software.

307.5 - 4.7 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.

DETROIT POLICE DEPARTMENT

MANUAL

307.5 Facial Recognition

307.5 - 4.8 Probe Image

An unknown image captured for facial recognition.

307.5 - 4.9 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 - 4.10 Unsolved Image File

A probe image of an unknown suspect that may be added to an unidentified photo file if there is probable cause to believe that suspect has committed a felony. Photos in this file are searched against new mug shot enrollments and future face recognition probe images in an attempt to identify the photo suspect. Once the individual has been identified, the image shall be removed from the file.

307.5 - 4.11 User

An individual who is authorized to access the SNAP application and whose agency is approved by the Michigan Department of State Police (MSP) to utilize the SNAP.

307.5 - 5 Governance and Oversight

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:

307.5 Facial Recognition

- 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 Acquiring and Receiving Facial Recognition Information

1. The Detroit Police Department's facial recognition system can access and perform facial recognition searches utilizing all entity-owned facial image repositories.
2. The Detroit Police Department is authorized to access and perform facial recognition searches utilizing the Statewide Network of Agency Photos (SNAP). These may include the following:
 - a. Mug shot images;
 - b. Driver's license photographs;
 - c. State identification card photographs; and
 - d. Sex Offender Registry.
3. For the purpose of performing facial recognition searches, authorized Department members will obtain probe images or accept probe images from authorized agencies for uses identified in this directive under section "Security and Maintenance."
4. Probe images will only be received from authorized law enforcement agencies in accordance with current memorandums of understanding established between this Department and the authorized entity involved. If a non-law enforcement entity wishes to submit a probe image for the purpose of a facial recognition search, the entity will be required to file an incident report with the appropriate law enforcement entity prior to the search.

DETROIT POLICE DEPARTMENT

MANUAL

307.5 Facial Recognition

5. The Detroit Police Department and, if applicable, any authorized requesting or participating agencies 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.
6. However, the Detroit Police Department accords special consideration to the collection of facial images relating to First Amendment-protected events, activities, and affiliations. Because of the sanctity of the First Amendment, law enforcement's role at First Amendment-protected events is usually limited to crowd control and public safety. If, however, during the planning assessment and approval process for the particular event, before proceeding with the collection, the DPD anticipates a need for the collection of facial images, the member assigned to vetting the event shall submit an Inter-Office Memorandum (DPD568), through channels, to the Department's Legal Advisor. The Inter-Office Memorandum (DPD568) shall include the legal or justified basis for such collection (including specifics regarding the criminal behavior that is suspected); and how facial images may be collected, used, or retained, in accordance with this policy, as appropriate. If facial images will be collected, the plan will specify the type of information collection that is permissible, identify who will collect facial images (uniform or plainclothes members), and define the permissible acts of collection. Thereafter, the Legal Advisor will make a recommendation as to whether collection of facial images by law enforcement officers at the event is permissible and will forward the recommendation to the Chief of Police or their designee.
7. The use of mobile facial image capture devices relating to First Amendment-protected events, activities, and affiliations shall only be authorized by the Chief of Police, or designee, in advance of the event. Facial images from a First Amendment-protected event will be used in exigent circumstances when the public safety mission changes or when it is in support of an active or ongoing criminal or homeland security investigation that occurs during or resulted from a First Amendment-protected event. When the Chief of Police or their designee authorizes such use, the Board of Police Commissioners will be notified after such use.

307.5 - 7 Use of Facial Recognition Technology

307.5 - 7.1 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 (robbery,

307.5 Facial Recognition

sexual assault, homicide, or aggravated assault), home invasion investigation or a homeland security investigation.

307.5 - 7.2 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, home invasion investigation or a homeland security investigation.

307.5 - 7.3 Process for Requesting Facial Recognition and Comparison

1. Requests for facial recognition services shall be submitted to the Crime Intelligence Unit, with photograph(s) or video(s) to be reviewed, the incident number, the crime type, and other pertinent information.
2. If the examiner detects an investigative lead, the Crime Intelligence Unit shall complete a supplemental incident report for the requestor. The supplemental incident report shall contain the steps taken to compare the probe images and candidate images and how the examiner came to their conclusion.
3. In the event that a viable candidate cannot be located from examining the facial recognition candidate images, the requestor will be notified that no candidate was identified.
4. If the Crime Intelligence Unit cannot discern a viable candidate, the photograph of the suspect will be removed from the facial recognition system.

307.5 - 8 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:

DETROIT POLICE DEPARTMENT

MANUAL

307.5 Facial Recognition

- 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, agency, and contact information of the law enforcement user;
 - b. The date and time of access;
 - c. Case number;

307.5 Facial Recognition

- d. Probe images;
- e. The specific information accessed;
- f. The modification or deletion, if any, of the facial recognition information; and
- g. The authorized law enforcement or public safety justification for access (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number if available.

307.5 - 9 Accountability and Enforcement**307.5 - 9.1 Transparency**

1. The Department will be open with the public with regard to facial recognition information collection, receipt, access, use, dissemination, retention, and purging practices.
2. The Department's facial recognition administrator (LASO) will be responsible for reviewing and responding to inquiries and complaints about the entity's use of facial recognition system, as well as complaints regarding incorrect information or privacy, civil rights, and civil liberties protections of the image repository maintained and facial recognition system accessed by the Department.
3. The Department will submit monthly reports 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.

307.5 - 9.2 Accountability

1. The Department will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the facial recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to facial recognition information, may include any type of medium or technology (e.g. physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least monthly, and a record of the audits will be maintained by the facial recognition administrator pursuant to the retention policy. Audits may be complete by an independent third party or a designated representative. Appropriate elements of this audit process a key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.
 2. Department members or other authorized users shall report errors, malfunctions, or deficiencies of facial recognition information and suspected or confirmed violations of the Department's facial recognition policy to the facial recognition administrator.
 3. The facial recognition administrator will review and update the provisions contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the facial recognition system; the audit review; and public expectations.
-
-

DETROIT POLICE DEPARTMENT

MANUAL

307.5 Facial Recognition

307.5 - 9.3 Discipline

- 1. 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. Suspended or discontinued access to information;**
 - b. Appropriate disciplinary or administrative actions or sanctions; and/or**
 - c. Referred to the appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.**

- 2. 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.**

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.

APPROVED
JUL 25 2019
SECOND DEPUTY CHIEF
POLICE LEGAL ADVISOR

APPROVED
ADMINISTRATIVE CHIEF
ADMINISTRATIVE OPERATIONS

RECEIVED
JUL 25 2019
BOARD OF POLICE COMMISSIONERS

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

307.5 Facial Recognition**307.5 - 4.2 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 - 4.3 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 1 investigation.

307.5 - 4.4 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.
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.
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.
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 from the facial recognition system.

307.5 - 5 Governance and Oversight**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.



INTER-OFFICE MEMORANDUM

To: Chairperson Lisa Carter, Board of Police Commissioners
Vice-Chairperson Eva Garza Dewaelsche, Board of Police Commissioners
Commissioner Willie E. Bell, Immediate Past Chairperson, Board of Police Commissioners
Honorable Board of Police Commissioners

From: Mr. Gregory Hicks, Secretary to the Board of Police Commissioners
Melanie A. White, Executive Manager of Policy, Board of Police Commissioners

Date: Thursday, September 5, 2019

Re: Board of Police Commissioners' ('Board') Policy Division Memorandum on Policy Recommendations for **Facial Recognition 307.5**

Introduction:

In 2017, the Detroit Police Department (hereinafter 'Department' or 'DPD') contracted for Facial Recognition with Data Works Plus Company. Subsequently, Detroit City Council approved the contract, and the Department has operated with the technology system for almost two years.

On January 18, 2019, the Detroit Police Department transmitted its first version of the proposed policy on Facial Recognition for the Board of Police Commissioners' (hereinafter 'Board') consideration.

On June 27, 2019, the Department rescinded the first version of the Facial Recognition proposed policy for "technical refinements" and indicated that it would return a revised policy version for the Board's consideration, specifically eliminating the surveillance or live video streaming component of Facial Recognition along with other areas.

On August 1, 2019, the Department transmitted the revised Facial Recognition Policy. The Department also indicated their willingness to engage in a discussion and refinement to the proposed Facial Recognition policy.

The Honorable Board of Police Commissioners requested the Policy Division to conduct a review of the proposed policies (both versions) and identify policy recommendations.



CITY OF DETROIT
BOARD OF POLICE COMMISSIONERS

DETROIT PUBLIC SAFETY HEADQUARTERS
1301 THIRD STREET, SUITE 767
DETROIT, MI 48226
TELEPHONE: 313-596-2430
FAX#: 313-596-1830
WWW.DETROITMI.GOV

The Policy Division conducted a robust review and evaluation of professional guidelines and recommendations for the Facial Recognition policy. The Policy Division further attended the Department's Real Time Crime Center ('RTCC') Facial Recognition Tour, and spoke with Department Executives. Additionally, the Division engaged in reviews and communications with various officials from jurisdictions and agencies around the country on the subject matter. Lastly, we attended the weekly Board of Police Commissioners' meetings, noted the Board's, public's concerns and feedback, as well as the Department's comments. All of the above activity helped develop the recommendations listed below. See references below.

The following policy recommendations are submitted for the Board's (committee of the whole) consideration. The recommendations are divided into two categories: 1. *Broad Category* and 2. *Critical Importance Category*.

The policy recommendations encompass reviews of both proposed policies. Please note that within this document, recommendations entitled "NEW" reflect a Board proposed recommendation. Recommendations entitled "UPDATED" consist of a provision already contained in the Department's proposed policy but was either revised or reemphasized for the Board's attention.



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

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

1. **NEW:** Specific Purpose of the Facial Recognition Technology 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. "(a) Face recognition refers to an automated process of matching face images utilizing algorithms and biometric scanning technologies [and human component review].¹
 - ii. (b) The system aids in the support of an ongoing Part 1 Violent Crime Investigation or a Home Invasion I investigation.²
 - iii. Part 1 Violent Crimes: Criminal Homicides, Sexual Assaults, Aggravated Assaults, Non-Fatal Shootings; Robberies, and Carjacking.
 - iv. Home Invasion I Elements:
 1. (1) entered a home without permission or broke in,
 2. (2) intended to commit or did commit a felony, larceny, or assault in the home, and
 3. (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. (c) 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.
2. **NEW:** 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 (i.e. FBI Agency, Department-Approved Training, other nationally recognized Facial Recognition conferences, etc.).

¹ Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America* (Oct. 16, 2016), <https://www.perpetuallineup.org/recommendations>.

² *Id.*



3. **NEW:** 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.).
4. **NEW:** Indicate Minimum Required 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 section)
 - 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.”
5. **UPDATED:** 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. Biometric Data
 - b. Data Works 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 policy³:

- 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

³ *Id.* (See also The Center for Catastrophe Preparedness & Response).



Police Department and the Michigan Department of State (MSP) to utilize the SNAP.⁴

- 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."⁵
- 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."⁶

Please cite whether the following terms will be applicable regarding the use of the Facial Recognition System:

- a. False negative: "An incorrect non-match between a probe and a candidate in the gallery returned by a face recognition algorithm, technology, or system."⁷
- b. False positive: "An incorrect match between a biometric probe and biometric template returned by a face recognition during the verification task."⁸
- c. False reject: "An incorrect non-match between a biometric probe and biometric template returned by a face recognition during the verification task."⁹
- d. False reject rate: "A statistic used to measure biometric performance when performing the verification task. The percentage of times a face 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."¹⁰
- e. Identification: "A task where the biometric system searches a database for a biometric template that matches a submitted

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*



biometric sample (probe), and if found, returns a corresponding identity."¹¹

6. **NEW:** Address Data Retention Area: The Department shall address any applicable Data Retention Requirements within the proposed directive.
 - a. I.e. 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, etc.).
7. **NEW:** 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.
8. **UPDATED:** 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. **UPDATED:** 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 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

¹¹ *Id.*



CITY OF DETROIT
BOARD OF POLICE COMMISSIONERS

DETROIT PUBLIC SAFETY HEADQUARTERS
1301 THIRD STREET, SUITE 767
DETROIT, MI 48226
TELEPHONE: 313-596-2430
FAX#: 313-596-1830
WWW.DETROITMI.GOV

be made available upon request for review and inspection by
the Board of Police Commissioners.



Critical Importance Category: Addresses Specific areas of importance such as required notifications, required audits, and required prohibitions.

Required Notifications:

9. **NEW:** 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 scheduled 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.
10. **NEW:** 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.
11. **NEW:** Notification of Algorithm Agnostic Upgrade, Improvements, or Changes: The Department shall immediately notify the Board of Police Commissioners of all algorithm agnostic upgrades, improvements, or changes with the Facial Recognition System.
12. **NEW:** 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."
13. **NEW:** 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.

Required Audits/Documentation:

14. **UPDATED:** *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 and 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.
15. **NEW:** *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.
 - a. 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?
 - b. Whether the Department allows a third party agency to conduct the auditing?
 - c. Whether the Department will engage in its own auditing measures? What will be the processes?
 - d. The percentage rate of identifying Part I Violent Crime offenders.
16. **UPDATED:** *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. *Revised:* The Department shall immediately inform the Board of Police Commissioners in writing of all Enforcement Actions and alleged offending personnel involved.

17. **UPDATED:** Specify Annual Report Mandatory Provisions 307.5 – 5.3: 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 judgment, 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 rights 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.

18. **UPDATED:** 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.~~



Required Prohibitions:

19. **NEW:** *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 but shall only be used as an investigative lead.
- e. Recommended language: "The information provided does not constitute probable case for an arrest. The results are only possible names(s) 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."
20. **NEW:** *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.
21. **NEW:** *Prohibition against Facial Recognition for Immigration Purposes:* The DPD shall be prohibited from the use of Facial Recognition for 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.
22. **NEW:** *Predictive Analytics Prohibited.* The Department shall be prohibited from using Predictive Analytics through the use of Facial Recognition Technology. Predictive Analysis 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.
23. **UPDATED:** *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 solely on the following:



CITY OF DETROIT
BOARD OF POLICE COMMISSIONERS

DETROIT PUBLIC SAFETY HEADQUARTERS
1301 THIRD STREET, SUITE 767
DETROIT, MI 48226
TELEPHONE: 313-596-2430
FAX#: 313-596-1830
WWW.DETROITMI.GOV

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



References:

1. U.S. Const. amend. I.
2. U.S. Const. amend. IV.
3. U.S. Const. amend. XIV.
4. 2019 HB 4810.
5. 2019 SB 342.
6. Detroit Police Department Proposed Policy on Facial Recognition January 18, 2019.
7. Detroit Police Department Revised Proposed Policy on Facial Recognition June 27, 2019.
8. Mayor Michael E. Duggan: "I Oppose the Use of Facial Recognition Technology for Surveillance." 18 Jul 2019.
<https://detroitmi.gov/news/mayor-duggan-i-oppose-use-facial-recognition-technology-surveillance>.
9. San Francisco, California, Municipal Code § 190110.
10. Berkley, California, Municipal Code § 2.99.
11. Somerville, Massachusetts, Municipal Code § 2019-16.
12. Councilmember Kate Harrison. "Adopt an Ordinance Amending Berkley Municipal Code Chapter 2.99 to Prohibit City Use of Face Recognition Technology." 11 Jun. 2019, 20-23.
13. City of Somerville Massachusetts. *Banning the usage of facial recognition technology in Somerville*. 9 May 2019. 24 Jun 2019. 27 June 2019.
14. City of Berkeley. *Peace and Justice Commission Meeting Regular Meeting*. 3 Jun 2019.
15. Crockford, Kade and Falcon, Emillano. "Ordinance Banning the Use of Facial Recognition Technology in Somerville." 17 Jun. 2019. 1-8.
16. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Face Recognition in America* (Oct. 16, 2016),
<https://www.perpetuallineup.org/recommendations>.
 - a. Georgetown Law. Center on Technology & Privacy. *The Perpetual Line-Up XII. Model Face Recognition Use Policy*,
<https://www.perpetuallineup.org/recommendations>.
17. Garvie, Clare and Moy, Laura M., *America Under Watch Face Surveillance in the United States*,
<https://www.americaunderwatch.com/#detroit>.
18. ACLU Sample Ordinance entitled "*An Act to Promote Transparency, the Public's Welfare, Civil Rights, and Civil Liberties in All Decisions Regarding the Funding, Acquisition, and Deployment of Military and Surveillance Equipment*," October 2018.



19. ACLU Sample Ordinance entitled "*An Act to Promote Transparency and Protect Civil Rights and Civil Liberties with Respect to Surveillance Technology*" October 2018.
20. ACLU Chicago Report, *Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to our Privacy*, ACLU of Illinois, February 2011.
21. Smith, Brad. *Facial Recognition: Coming to a Street Near You*. <https://www.brookings.edu/events/facial-recognition-coming-to-a-street-corner-near-you/>.
22. Ozer & Bibring, 2016. *Making Smart Decisions about Surveillance, a Guide for Community Transparency, Accountability, & Oversight*, the ACLU of California.
23. The Conversation. *Emotion-reading tech fails the racial bias test*. Jan. 3, 2019.
24. McCullom, Rod. *Facial Recognition Technology is Both Biased and Understudied*. May 17, 2019.
25. Automated Regional Justice Information (System) (ARJIS Acceptable Use Policy for Facial Recognition).
26. Baltimore Police Department, *Video Surveillance Procedures, Policy 1014*, August 1, 2016.
27. Metropolitan Police Department, *Surveillance Policies and Procedures*, <https://mpdc.dc.gov/node/214522>.
28. Honolulu Police Department Policy Auxiliary and Technical Services.
29. New York City Council Bill Int. No. 487. (3), <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0>.
30. *Face Off Law Enforcement Use of Face Recognition Technology*, Jennifer Lynch, Senior Staff Attorney, Electronic Frontier Foundation, February 2018.
31. Ratcliffe, Jerry. *Video Surveillance of Public Places*, Center for Problem-Oriented Policing, Response Guides Series Problem-Oriented Guides for Police, No. 4, August 2011.
32. La Vigne, Nancy G. et. al., 2011. *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention—A Summary*, Urban Institute Justice Police Center.
33. Egan, Paul. *Never arrested? Michigan State Police still likely has your photo in its database*. (March 11, 2019). <https://www.freep.com/story/news/local/michigan/2019/03/11/michigan-state-police-facial-recognition-database/3102139002/>.



34. You Could Be a Victim of Negligence by Michigan State Police, Published on March 18, 2019, <https://www.thurswell.com/victim-negligence-michigan-state-police/>.
35. Bala, Nila and Watney, Caleb. *What Are the Proper Limits on Police Use of Facial Recognition?*
<https://www.brookings.edu/blog/techtank/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition/>.
36. World Population Review, <http://worldpopulationreview.com/us-cities/detroit-population/>.
37. Matthew Feeney, Cato Institute.
38. Proposed City Ordinance, *Article II, Police Department, Division 3, Community Control Over Police Surveillance; Sections 43-2-31 through 43-2-42.*
39. CCOPS Section 8. Community Advisory Committee on Surveillance.
40. Electronic Surveillance: Part B: Technologically-Assisted Physical Surveillance,
https://www.americanbar.org/groups/criminal_justice/publications/criminal_justice_section_archive/crimjust_standards_tabs_blk/, June 30, 2017.
41. Civil Rights Coalition Opposes Facial Recognition Technology in Letter to Detroit Board of Police Commissioners.
42. Detroit Police Department Professional Services Contract between City of Detroit, Michigan and DataWorks Plus Contract No. 6000801.



1 [Administrative Code - Acquisition of Surveillance Technology]

2

3 **Ordinance amending the Administrative Code to require that City departments**
 4 **acquiring Surveillance Technology submit a Board of Supervisors approved**
 5 **Surveillance Technology Policy Ordinance and a Surveillance Impact Report to the**
 6 **Board in connection with any request to appropriate funds for the purchase of such**
 7 **technology or to accept and expend grant funds for such purpose, or otherwise to**
 8 **procure Surveillance Technology equipment or services; require each City department**
 9 **that owns and operates existing surveillance technology equipment or services to**
 10 **submit to the Board a proposed Surveillance Technology Policy Ordinance governing**
 11 **the use of the surveillance technology; and requiring the Controller, as City Services**
 12 **Auditor, to audit annually the use of surveillance technology equipment or services**
 13 **and the conformity of such use with an approved Surveillance Technology Policy**
 14 **Ordinance and provide an audit report to the Board of Supervisors.**

15 **NOTE:** **Unchanged Code text and uncodified text** are in plain Arial font.
 16 **Additions to Codes** are in *single-underline italics Times New Roman font*.
 17 **Deletions to Codes** are in ~~*italics Times New Roman font*~~.
 18 **Board amendment additions** are in double-underlined Arial font.
 19 **Board amendment deletions** are in ~~Arial font~~.
 20 **Asterisks (* * * *)** indicate the omission of unchanged Code
 21 subsections or parts of tables.

22 Be it ordained by the People of the City and County of San Francisco:

23 Section 1. General Findings.

24 (a) It is essential to have an informed public debate as early as possible about
 25 decisions related to surveillance technology.

1 (b) Whenever possible, decisions relating to surveillance technology should occur with
2 strong consideration given to the impact such technologies may have on civil rights and civil
3 liberties, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments
4 to the United States Constitution as well as Sections 1, 2, and 13 of Article I of the California
5 Constitution.

6 (c) While surveillance technology may threaten the privacy of all of us, surveillance
7 efforts have historically been used to intimidate and oppress certain communities and groups
8 more than others, including those that are defined by a common race, ethnicity, religion,
9 national origin, income level, sexual orientation, or political perspective.

10 (d) The propensity for facial recognition technology to endanger civil rights and civil
11 liberties substantially outweighs its purported benefits, and the technology will exacerbate
12 racial injustice and threaten our ability to live free of continuous government monitoring.

13 (e) Whenever possible, decisions regarding if and how surveillance technologies
14 should be funded, acquired, or used, and whether data from such technologies should be
15 shared, should be made only after meaningful public input has been solicited and given
16 significant weight.

17 (f) Legally enforceable safeguards, including robust transparency, oversight, and
18 accountability measures, must be in place to protect civil rights and civil liberties before any
19 surveillance technology is deployed; and

20 (g) If a surveillance technology is approved, data reporting measures must be adopted
21 that empower the Board of Supervisors and the public to verify that mandated civil rights and
22 civil liberties safeguards have been strictly adhered to.

23 ///

24 ///

25

1 Section 2. The Administrative Code is amended by adding Chapter 19B, consisting of
2 Sections 19B.1-19B.8, to read as follows:

3
4 **CHAPTER 19B: ACQUISITION OF SURVEILLANCE TECHNOLOGY**

5
6 **SEC. 19B.1. DEFINITIONS.**

7 "Annual Surveillance Report" means a written report that includes all of the following:

8 (1) A general description of how the Surveillance Technology was used;

9 (2) A general description of whether and how often data acquired through the use of the
10 Surveillance Technology item was shared with outside entities, the name of any recipient outside entity,
11 the type(s) of data disclosed, under what legal standard(s) the data was disclosed, and the justification
12 for the disclosure(s);

13 (3) A summary of complaints or concerns from the public about the Surveillance
14 Technology item;

15 (4) The aggregate results of any internal audits required by the Surveillance Technology
16 Policy, any general, aggregate information about violations of the Surveillance Technology Policy, and
17 a general description of any actions taken in response;

18 (5) Information, including crime statistics, which help the Board of Supervisors assess
19 whether the Surveillance Technology has been effective at achieving its identified purposes;

20 (6) Aggregate statistics and information about any Surveillance Technology related to
21 Public Records Act requests;

22 (7) Total annual costs for the Surveillance Technology, including personnel and other
23 ongoing costs, and what source of funding will fund the Surveillance Technology in the coming year;

24 (8) Any requested modifications to the Surveillance Technology Policy and a detailed
25 basis for the request;

1 (9) Where applicable, a general breakdown of what physical objects the Surveillance
2 Technology hardware was installed upon, using general descriptive terms; for Surveillance Technology
3 software, a general breakdown of what data sources the Surveillance Technology was applied to; and

4 (10) A summary of all requests for Board of Supervisors' approval for a Surveillance
5 Technology Policy ordinance.

6 An Annual Surveillance Report shall not contain the specific records that a Surveillance
7 Technology item collects, stores, exchanges, or analyzes and/or information protected, restricted,
8 and/or sealed pursuant to State and/or federal laws, including information exempt from disclosure
9 under the California Public Records Act.

10 "City" means the City and County of San Francisco.

11 "City Department" or "Department" means any City official, department, board, commission,
12 or other entity in the City except that it shall not mean the District Attorney or Sheriff when performing
13 their investigative or prosecutorial functions, provided that:

14 (1) The District Attorney or Sheriff certifies in writing to the Controller that acquisition
15 of Surveillance Technology is necessary to perform an investigative or prosecutorial function, and

16 (2) The District Attorney or Sheriff provides in writing to the Controller either an
17 explanation of how compliance with this Chapter 19B will obstruct their investigative or prosecutorial
18 function or a declaration that the explanation itself will obstruct either function.

19 "Exigent circumstances" means an emergency involving imminent danger of death or serious
20 physical injury to any person that requires the immediate use of Surveillance Technology or the
21 information it provides.

22 "Face recognition" means an automated or semi-automated process that assists in identifying
23 or verifying an individual based on an individual's face.

24 "Surveillance Impact Report" means a written report that includes at a minimum the following:

25

1 (1) Information describing the Surveillance Technology and how it works, including
2 product descriptions from manufacturers;

3 (2) Information on the proposed purpose(s) for the Surveillance Technology;

4 (3) If applicable, the general location(s) it may be deployed and crime statistics for any
5 location(s);

6 (4) An assessment identifying any potential impact on civil liberties and civil rights and
7 discussing any plans to safeguard the rights of the public;

8 (5) The fiscal costs for the Surveillance Technology, including initial purchase,
9 personnel and other ongoing costs, and any current or potential sources of funding;

10 (6) Whether use or maintenance of the technology will require data gathered by the
11 technology to be handled or stored by a third-party vendor on an ongoing basis; and

12 (7) A summary of the experience, if any, other governmental entities have had with the
13 proposed technology, including information about its effectiveness and any known adverse information
14 about the technology such as unanticipated costs, failures, or civil rights and civil liberties abuses.

15 "Personal communication device" means a cellular telephone that has not been modified
16 beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or
17 similar wireless two-way communications and/or portable Internet accessing devices, whether
18 procured or subsidized by a City entity or personally owned, that is used in the regular course of
19 conducting City business.

20 "Surveillance Technology" means any software, electronic device, system utilizing an
21 electronic device, or similar device used, designed, or primarily intended to collect, retain, process, or
22 share audio, electronic, visual, location, thermal, biometric, olfactory or similar information
23 specifically associated with, or capable of being associated with, any individual or group. Surveillance
24 Technology" includes but is not limited to the following: international mobile subscriber identity
25 (IMSI) catchers and other cell site simulators; automatic license plate readers; electric toll readers;

1 closed-circuit television cameras; gunshot detection hardware and services; video and audio
2 monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and
3 wearable body cameras; mobile DNA capture technology; biometric software or technology, including
4 facial, voice, iris, and gait-recognition software and databases; software designed to monitor social
5 media services; x-ray vans; software designed to forecast criminal activity or criminality; radio-
6 frequency I.D. (RFID) scanners; and tools, including software and hardware, used to gain
7 unauthorized access to a computer, computer service, or computer network. Surveillance Technology
8 does not include the following devices, hardware, or software:

9 (1) Office hardware, such as televisions, computers, credit card machines, copy
10 machines, telephones, and printers, that are in common use by City Departments and used for routine
11 City business and transactions;

12 (2) City databases and enterprise systems that contain information kept in the ordinary
13 course of City business, including, but not limited to, human resource, permit, license, and business
14 records;

15 (3) City databases and enterprise systems that do not contain any data or other
16 information collected, captured, recorded, retained, processed, intercepted, or analyzed by
17 Surveillance Technology, including payroll, accounting, or other fiscal databases;

18 (4) Information technology security systems, including firewalls and other cybersecurity
19 systems intended to secure City data;

20 (5) Physical access control systems, employee identification management systems, and
21 other physical control systems;

22 (6) Infrastructure and mechanical control systems, including those that control or
23 manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;

1 (7) Manually-operated technological devices used primarily for internal City
2 communications, which are not designed to surreptitiously collect surveillance data, such as radios,
3 personal communication devices, and email systems;

4 (8) Manually-operated and non-wearable handheld cameras, audio recorders, and video
5 recorders, that are not designed to be used surreptitiously and whose functionality is limited to
6 manually capturing and manually downloading video and/or audio recordings;

7 (9) Surveillance devices that cannot record or transmit audio or video or be remotely
8 accessed, such as image stabilizing binoculars or night vision equipment;

9 (10) Computers, software, hardware, or devices, used in monitoring the work and work-
10 related activities involving City buildings, employees, contractors, and volunteers or used in
11 conducting internal investigations involving City employees, contractors, and volunteers;

12 (11) Medical equipment and systems used to record, diagnose, treat, or prevent disease
13 or injury, and used and/or kept in the ordinary course of providing City services;

14 (12) Parking Ticket Devices;

15 (13) Police Department interview rooms, holding cells, and internal security
16 audio/video recording systems;

17 (14) Police department computer aided dispatch (CAD), records/case management, Live
18 Scan, booking, Department of Motor Vehicles, California Law Enforcement Telecommunications
19 Systems (CLETS), 9-1-1 and related dispatch and operation or emergency services systems;

20 (15) Police department early warning systems; and

21 (16) Computers, software, hardware, or devices used to monitor the safety and security
22 of City facilities and their occupants.

23 "Surveillance Technology Policy" means a written policy that includes:

24 (1) A description of the product and services addressed by the Surveillance Technology,
25 including manufacturer and model numbers and/or the identity of any provider(s) whose services are

1 essential to the functioning or effectiveness of the Surveillance Technology equipment or services for
2 the intended purpose:

3 (2) A description of the purpose(s) for which the Surveillance Technology equipment or
4 services are proposed for acquisition, including the type of data that may be collected by the
5 Surveillance Technology equipment or services:

6 (3) The uses that are authorized, the rules and processes required prior to such use, and
7 uses of the Surveillance Technology that will be expressly prohibited.

8 (4) A description of the formats in which information collected by the Surveillance
9 Technology is stored, copied, and/or accessed:

10 (5) The specific categories and titles of individuals who are authorized by the
11 Department to access or use the collected information, including restrictions on how and under what
12 circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the
13 rules and processes required prior to access or use of the information:

14 (6) The general safeguards that protect information from unauthorized access, including
15 encryption and access control mechanisms:

16 (7) The limited time period, if any, that information collected by the Surveillance
17 Technology will be routinely retained, the reason such retention period is appropriate to further the
18 purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is
19 regularly deleted after that period lapses, and the specific conditions that must be met to retain
20 information beyond that period:

21 (8) How collected information can be accessed or used by members of the public,
22 including criminal defendants:

23 (9) Which governmental agencies, departments, bureaus, divisions, or units that may
24 receive data collected by the Surveillance Technology operated by the Department, including any

25

1 required justification or legal standard necessary to share that data and how it will ensure that any
2 entity receiving such data complies with the Surveillance Technology Policy;

3 (10) The training required for any individual authorized to use the Surveillance
4 Technology or to access information collected by the Surveillance Technology;

5 (11) The mechanisms to ensure that the Surveillance Technology Policy is followed,
6 including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of
7 the use of the technology or access to information collected by the technology, technical measures to
8 monitor for misuse, any independent person or entity with oversight authority, and the sanctions for
9 violations of the policy; and

10 (12) What procedures will be put in place by which members of the public can register
11 complaints or concerns, or submit questions about the deployment or use of a specific Surveillance
12 Technology, and how the Department will ensure each question and complaint is responded to in a
13 timely manner.

14
15 **SEC. 19B.2. BOARD OF SUPERVISORS APPROVAL OF SURVEILLANCE**
16 **TECHNOLOGY POLICY.**

17 (a) Except as stated in subsection (c), a Department must obtain Board of Supervisors approval
18 by ordinance of a Surveillance Technology Policy under which the Department will acquire and use
19 Surveillance Technology, prior to engaging in any of the following:

20 (1) Seeking funds for Surveillance Technology, including but not limited to applying for
21 a grant, or accepting state or federal funds, or public or private in-kind or other donations;

22 (2) Acquiring or borrowing new Surveillance Technology, including but not limited to
23 acquiring Surveillance Technology without the exchange of monies or other consideration;

1 (3) Using new or existing Surveillance Technology for a purpose, in a manner, or in a
2 location not specified in a Surveillance Technology Policy ordinance approved by the Board in
3 accordance with this Chapter 19B; or

4 (4) Entering into agreement with a non-City entity to acquire, share, or otherwise use
5 Surveillance Technology.

6 (b) Notwithstanding the provisions of this Chapter 19B, it shall be unlawful for any Department
7 to obtain, retain, access, or use: 1) any Face Recognition Technology; or 2) any information obtained
8 from Face Recognition Technology.

9 (c) If either the District Attorney or Sheriff certifies in writing to the Controller that acquisition
10 of Surveillance Technology is necessary to perform an investigative or prosecutorial function and
11 provides in writing to the Controller either an explanation of how compliance with this Chapter 19B
12 will obstruct their investigative or prosecutorial function or a declaration that the explanation itself
13 will obstruct either function, the District Attorney or Sheriff shall simultaneously submit a copy of the
14 document to the Clerk of the Board of Supervisors so that the Board in its discretion may hold a
15 hearing and request that the District Attorney or Sheriff appear to respond to the Board's questions
16 regarding such certification, explanation, and/or declaration.

17 (d) Nothing in this Chapter 19B shall be construed to obstruct the constitutional and statutory
18 powers and duties of the District Attorney, the Sheriff, the Chief Adult Probation Officer, or the Chief
19 Juvenile Probation Officer.

20
21 **SEC. 19B.3. SURVEILLANCE IMPACT REPORT AND SURVEILLANCE TECHNOLOGY**
22 **POLICY SUBMISSION.**

23 (a) The Department seeking approval under Section 19B.2 shall submit to the Board of
24 Supervisors and publicly post on the Department website a Surveillance Impact Report and a proposed
25

1 Surveillance Technology Policy ordinance at least 30 days prior to the public meeting where the Board
2 will consider that Surveillance Technology Policy ordinance pursuant to Section 19B.2.

3 (b) Prior to submitting the Surveillance Technology Policy ordinance to the Board, the
4 Department must first approve the policy, submit the policy to the City Attorney for review, and submit
5 the policy to the Mayor.

6
7 **SEC. 19B.4. STANDARD FOR APPROVAL.**

8 It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy
9 ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes
10 outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and
11 civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will
12 not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any
13 community or group.

14
15 **SEC. 19B.5. COMPLIANCE FOR EXISTING SURVEILLANCE TECHNOLOGY.**

16 (a) Each Department possessing or using Surveillance Technology before the effective date of
17 this Chapter 19B shall submit a proposed Surveillance Technology Policy ordinance to the Board of
18 Supervisors for that particular Surveillance Technology no later than 120 days following the effective
19 date of this Chapter, for review and approval by the Board by ordinance.

20 (b) If a Department is unable to meet this 120-day timeline, the Department may notify the
21 Clerk of the Board of Supervisors in writing of the Department's request to extend this period and the
22 reasons for that request. The Clerk of the Board may for good cause grant a Department a single
23 extension of up to 90 days beyond the 120-day timeline to submit a proposed Surveillance Technology
24 Policy.

1 (c) If the Board has not approved a Surveillance Technology Policy ordinance for Surveillance
2 Technology in use before the effective date of this Chapter 19B, within 180 days of its submission to the
3 Board, the Department shall cease its use of the Surveillance Technology and the sharing of data from
4 the Surveillance Technology until such time as the Board approves the Surveillance Technology Policy
5 ordinance in accordance with this Chapter.

6
7
8 **SEC. 19B.6. ANNUAL SURVEILLANCE REPORT.**

9 (a) A Department that obtains approval for the acquisition of Surveillance Technology under
10 Section 19B.2 must submit to the Board of Supervisors, and make available on its website, an Annual
11 Surveillance Report for each Surveillance Technology used by the City Department within 12 months of
12 Board approval of the applicable Surveillance Technology Policy, and annually thereafter on or before
13 November 1. If the Department is unable to meet the deadline, the Department may submit a request to
14 the Clerk of the Board for an extension of the deadline. The Clerk may extend the deadline for good
15 cause.

16 (b) By no later than January 15 of each fiscal year, each Department that has obtained
17 approval for the acquisition of Surveillance Technology under Section 19B.2 shall submit to the Board
18 of Supervisors a report regarding implementation of the policy and a resolution to accept the report.

19 (c) By no later than January 15 of each year, the Board of Supervisors shall publish a summary
20 of all requests for Board approval of Surveillance Technology Policy ordinances, which shall include a
21 summary of any Board action related to such requests, and all Annual Surveillance Reports submitted
22 in the prior calendar year.

23
24 **SEC. 19B.7. USE OF SURVEILLANCE TECHNOLOGY IN EXIGENT**
25 **CIRCUMSTANCES.**

1 (a) A Department may temporarily acquire or temporarily use Surveillance Technology in
2 exigent circumstances without following the provisions of this Chapter 19B. If a Department acquires
3 or uses Surveillance Technology under this Section 19B.7, the Department shall do all of the following:

4 (1) Use the Surveillance Technology solely to respond to the exigent circumstances;

5 (2) Cease using the Surveillance Technology within seven days, or when the exigent
6 circumstances end, whichever is sooner;

7 (3) Keep and maintain only data related to the exigent circumstances, and dispose of
8 any data that is not relevant to an ongoing investigation, unless its retention is (A) authorized by a
9 court based on a finding of probable cause to believe the information constitutes evidence of a crime;
10 or (B) otherwise required by law;

11 (4) Not disclose to any third party any information acquired during exigent
12 circumstances unless such disclosure is (A) authorized by a court based on a finding of probable cause
13 to believe the information constitutes evidence of a crime; or (B) otherwise required by law; and

14 (5) Submit a written report summarizing that acquisition and/or use of Surveillance
15 Technology under this Section 19B.7 to the Board of Supervisors within 45 days following the inception
16 of the exigent circumstances.

17 (b) Any Surveillance Technology temporarily acquired in exigent circumstances shall be
18 returned within 7 days following its acquisition, or when the exigent circumstances end, whichever is
19 sooner, unless the Department acquires the Surveillance Technology in accordance with the
20 requirements of this Chapter 19B.

21
22 **SEC. 19B.8. ENFORCEMENT.**

23 (a) If a Department alleged to have violated this Chapter 19B takes corrective measures in
24 response to such allegation, the Department shall post a notice on the Department's website that
25 generally describes any corrective measure taken to address such allegation.

1 (b) It shall be a misdemeanor to knowingly use City-owned Surveillance Technology (1) for a
2 purpose or in a manner that is specifically prohibited in a Board-approved Surveillance Technology
3 Policy ordinance, or (2) without complying with the terms of this Chapter 19B. Unless otherwise
4 prohibited by law, the District Attorney may prosecute a violation of this Chapter.

5 (c) Any violation of this Chapter 19B constitutes an injury and any person may institute
6 proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent
7 jurisdiction to enforce this Chapter 19B. An action instituted under this subsection (c) shall be brought
8 against the City.

9 (d) Prior to the initiation of any legal proceeding under subsection (c), the City must be given
10 written notice of the violation(s) and an opportunity to correct such alleged violation(s) within 30 days
11 of receipt of the notice.

12 (e) If the alleged violation(s) is substantiated and subsequently corrected, a notice shall be
13 posted in a conspicuous space on the City's website that describes the corrective measure(s) taken to
14 address the violation(s).

15 (f) A court shall award costs and reasonable attorney's fees to a plaintiff who is a prevailing
16 party in any action brought under subsection (c).

17
18 Section 3. The Administrative Code is hereby amended by revising Sections 2A.20 and
19 10.170-1, and adding Sections 3.27 and 21.07, to read as follows:

20
21 **SEC. 2A.20. CONTROLLER'S AUDITS.**

22 (a) The Controller shall audit the accounts of all boards, officers, and employees of the
23 City and County charged in any manner with the custody, collection, or disbursement of funds.
24 The Controller shall audit all accounts of money coming into the hands of the Treasurer, the
25 frequency of which shall be governed by State law.

1 ***(b)*** The Controller shall have the authority to audit the operations of all boards,
2 commissions, officers, and departments to evaluate their effectiveness and efficiency. The
3 Controller shall have access to, and authority to examine all documents, records, books, and
4 other property of any board, commission, officer, or department.

5 ***(c)*** When requested by the Mayor, the Board of Supervisors, or any board or
6 commission for its own department, the Controller shall audit the accounts of any officer or
7 department.

8 ***(d) Surveillance Technology Audit.***

9 *(1) For purposes of this subsection (d), "Department," "Surveillance Technology,"*
10 *"Surveillance Technology Policy," and "Annual Surveillance Report" have the meanings set forth in*
11 *Section 19B.1 of the Administrative Code.*

12 *(2) Acting as City Services Auditor, and beginning in fiscal year 2019-2020, the*
13 *Controller shall audit annually the use of Surveillance Technology by Departments. Such an audit shall*
14 *include a review of whether a Department has operated and is operating in compliance with an*
15 *approved Surveillance Technology Policy ordinance, and has completed an Annual Surveillance*
16 *Report. The audit shall also include a review of the difference, if any, between the full cost of the*
17 *Surveillance Technology equipment and services included in the Surveillance Technology Policy and*
18 *the total annual costs for the Surveillance Technology included in the Annual Surveillance Report. At*
19 *the completion of the audit and in consultation with the City Attorney, the Controller shall recommend*
20 *any changes to any Surveillance Technology Policy ordinance and its implementation to the Board of*
21 *Supervisors.*

22
23 **SEC. 10.170-1. GRANT FUNDS – ACCEPTANCE AND EXPENDITURE.**
24
25

1 (a) Any department, board, or commission that seeks to accept and expend federal,
2 State, or other grant funds must comply with any applicable provisions of this Section 10.170-
3 1.

4 (b) The acceptance and expenditure of federal, State, or other grant funds in the
5 amount of \$100,000 or more is subject to the approval by resolution of the Board of
6 Supervisors. If, as a condition of the grant, the City is required to provide any matching funds,
7 those funds shall be included in determining whether the grant meets the \$100,000 threshold.
8 This subsection (b) shall also apply to an increase in a grant where the increase, alone or in
9 combination with any other previous increases to that grant, would raise the cumulative total
10 amount of the grant to \$100,000 or more. The department, board, or commission requesting
11 approval shall submit the following documents to the Board prior to its consideration:

12 (1) A proposed resolution approving the acceptance and expenditure of grant
13 funds, or a proposed ordinance as required under subsection (d), signed by the department
14 head, the Mayor or his or her designee, and the Controller;

15 (2) A completed "Grant Information Form." The Clerk of the Board shall prepare
16 the form; it shall include a disability access checklist, indirect cost recovery, and other
17 information as the Board of Supervisors may require;

18 (3) A copy of the grant application;

19 (4) A letter of intent to award the grant or acknowledgment of grant award from
20 the granting agency; and,

21 (5) A cover letter to the Clerk of the Board ~~of Supervisors~~ substantially conforming
22 to the specifications of the Clerk of the Board.

23 (c) Grants or Increases to Grants of Less Than \$100,000. The Controller may prescribe
24 rules for the acceptance and expenditure of federal, State, or other grant funds in amounts
25 less than \$100,000, or for increases to grants where the increase, alone or in combination

1 with any other previous increases to that grant, would not raise the cumulative total amount of
2 the grant to \$100,000 or more. The Controller may also prescribe rules for the acceptance
3 and expenditure of increases to grants, where the original grant or any subsequent increase
4 to the grant has been approved by the Board of Supervisors under subsection (b) or (d) and
5 where the latest increase would be in an amount less than \$50,000.

6 * * * *

7 (l) Surveillance Technology.

8 (1) For purposes of this subsection (l), "Department," "Surveillance Technology," and
9 "Surveillance Technology Policy" have the meanings set forth in Section 19B.1 of the Administrative
10 Code.

11 (2) Notwithstanding the provisions of subsections (b) and (c) above, when any City
12 official, Department, board, commission or other entity of the City (collectively, the "requesting
13 department") seeks authority to apply for, accept, or expend federal, State, or other grant funds in any
14 amount to purchase Surveillance Technology, the requesting department must submit a Surveillance
15 Technology Policy, approved by the Board of Supervisors in accordance with Chapter 19B of the
16 Administrative Code, to the Board of Supervisors with a request for authorization to accept and expend
17 grant funds.

18
19
20 **SEC. 3.27. APPROPRIATIONS FOR SURVEILLANCE TECHNOLOGY.**

21 (a) For purposes of this Section 3.27, "Department," "Surveillance Technology," and
22 "Surveillance Technology Policy" have the meanings set forth in Section 19B.1 of the Administrative
23 Code.

24 (b) To the extent that a Department seeks funding to acquire Surveillance Technology, the
25 Department shall transmit a Surveillance Technology Policy, approved by the Board of Supervisors in

1 accordance with Chapter 19B of the Administrative Code, with any budget estimate submitted to the
2 Controller in accordance with Section 3.3(a) or 3.15 of the Administrative Code. To the extent the
3 Mayor concurs in the funding request and the Surveillance Technology Policy, the Mayor shall include
4 the Surveillance Technology Policy with the proposed budget submitted to the Board of Supervisors in
5 accordance with Section 3.3(c) or (d) of the Administrative Code, or, in the case of a supplemental
6 appropriation, Section 3.15 of the Administrative Code.

7 **SEC. 21.07. ACQUISITION OF SURVEILLANCE TECHNOLOGY.**

8 (a) For purposes of this Section 21.07, "Department," "Surveillance Technology," and
9 "Surveillance Technology Policy" have the meanings set forth in Section 19B.1 of the Administrative
10 Code.

11 (b) Notwithstanding any authority set forth in this Chapter 21, neither the Purchaser nor any
12 Contracting Officer may acquire any Surveillance Technology unless the Board of Supervisors has
13 appropriated funds for such acquisition in accordance with the requirements of Chapter 19B of the
14 Administrative Code.

15 Section 3. Effective Date. This ordinance shall become effective 30 days after
16 enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the
17 ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board
18 of Supervisors overrides the Mayor's veto of the ordinance.

19
20 III

21 III

22 III

23 III

24 III

25

1 Section 4. Scope of Ordinance. In enacting this ordinance, the Board of Supervisors
2 intends to amend only those words, phrases, paragraphs, subsections, sections, articles,
3 numbers, punctuation marks, charts, diagrams, or any other constituent parts of the Municipal
4 Code that are explicitly shown in this ordinance as additions, deletions, Board amendment
5 additions, and Board amendment deletions in accordance with the "Note" that appears under
6 the official title of the ordinance.

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

APPROVED AS TO FORM:
DENNIS J. HERRERA, City Attorney

By: _____
JANA CLARK
Deputy City Attorney

n:\egana\as2019\1900073\01334300 docx



FILED
OFFICE OF THE CITY CLERK
OAKLAND

2018 APR 26 PM 3:03

APPROVED AS TO FORM AND LEGALITY

Amadi Sotel
CITY ATTORNEY'S OFFICE

AMENDED AT THE APRIL 24, 2018 PUBLIC SAFETY COMMITTEE

OAKLAND CITY COUNCIL

ORDINANCE NO. _____ C.M.S.

ORDINANCE ADDING CHAPTER 9.64 TO THE OAKLAND MUNICIPAL CODE ESTABLISHING RULES FOR THE CITY'S ACQUISITION AND USE OF SURVEILLANCE EQUIPMENT

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to the City of Oakland's ("City") acquisition and use of surveillance technology; and

WHEREAS, the City Council finds that, while the use of surveillance technology may threaten the privacy of all citizens, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective; and

WHEREAS, while acknowledging the significance of protecting the privacy of citizens, the City Council finds that surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes; and

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and

WHEREAS, the City Council finds that no decisions relating to the City's use of surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the California and United States Constitutions; and

WHEREAS, the City Council finds that any and all decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight in policy decisions; and

WHEREAS, the City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect civil rights and civil liberties before any City surveillance technology is deployed; and

WHEREAS, the City Council finds that if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF OAKLAND DOES ORDAIN AS FOLLOWS:

SECTION 1. This Ordinance shall be known as the Surveillance and Community Safety Ordinance.

SECTION 2. Oakland Municipal Code Chapter 9.64, is hereby added as set forth below (chapter and section numbers are indicated in **bold type**).

Chapter 9.64 REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

9.64.010. DEFINITIONS. The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:
 - A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
 - B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
 - C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such

- hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each Police Area in the relevant year;
 - E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.
 - F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.
 - G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
 - H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
 - I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
 - J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
 - K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.
2. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.
 3. "City staff" means City personnel authorized by the City Administrator or designee to seek City Council Approval of Surveillance Technology in conformance with this Chapter.
 4. "Continuing agreement" means an agreement that automatically renews unless terminated by one party.
 5. "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

6. "Large-scale event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.
7. "Personal communication device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.
8. "Police area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.
9. "Surveillance" or "surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.
10. "Surveillance technology" means any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.
 - A. "Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

1. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;
 2. Parking Ticket Devices (PTDs);
 3. Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;
 4. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
 5. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;
 6. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.
 7. Medical equipment used to diagnose, treat, or prevent disease or injury.
 8. Police department interview room cameras.
 9. Police department case management systems.
 10. Police department early warning systems.
 11. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above.
6. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:
- A. **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
 - B. **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
 - C. **Location:** The location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
 - D. **Impact:** An assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

- E. **Mitigations:** Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
 - F. **Data Types and Sources:** A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;
 - G. **Data Security:** Information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
 - H. **Fiscal Cost:** The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;
 - I. **Third Party Dependence:** Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;
 - J. **Alternatives:** A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
 - K. **Track Record:** A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).
7. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:
- A. **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance;
 - B. **Authorized Use:** The specific uses that are authorized, and the rules and processes required prior to such use;

- C. **Data Collection:** The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;
- D. **Data Access:** The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;
- E. **Data Protection:** The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;
- F. **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;
- G. **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants;
- H. **Third Party Data Sharing:** If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
- I. **Training:** The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;
- J. **Auditing and Oversight:** The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
- K. **Maintenance:** The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

9.64.020 Privacy Advisory Commission (PAC) Notification and Review Requirements

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

- A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:
 - 1. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,
 - 2. Soliciting proposals with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.

 - B. Upon notification by City staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, City staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action City staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the City staff modify the proposal, or take no action.

 - C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020.1.B, City staff may proceed and seek Council Approval of the proposed Surveillance Technology initiative pursuant to the requirements of Section 9.64.030.
2. PAC Review Required for New Surveillance Technology Before City Council Approval
- A. Prior to seeking City Council approval under Section 9.64.030, City staff shall submit a Surveillance Impact Report and a Surveillance Use Policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under 9.64.010.
 - B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to City staff. City staff shall present such

modifications to City Council when seeking City Council approval under Section 9.64.030.

- C. Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item.
3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval
- A. Prior to seeking City Council approval for existing City surveillance technology under Section 9.64.030 City staff shall submit a Surveillance Impact Report and Surveillance Use Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under 9.64.010.
 - B. Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, City staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the City.
 - C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.
 - D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020.1.C., City staff shall submit at least one (1) Surveillance Impact Report and proposed Surveillance Use Policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.
 - E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable City staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

9.64.030. City Council Approval Requirements for New and Existing Surveillance Technology.

- 1. City staff must obtain City Council approval prior to any of the following:

- A. Accepting state or federal funds or in-kind or other donations for surveillance technology;
- B. Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
- C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this ordinance; or
- D. Entering into a continuing agreement or written agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.
- E. Notwithstanding any other provision of this section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.

2. City Council Approval Process

- A. After the PAC Notification and Review requirements in Section 9.64.020 have been met, City staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed Surveillance Impact Report and proposed Surveillance Use Policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing.
- B. The City Council shall only approve any action as provided in this Chapter after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.
- C. For Approval of Existing Surveillance Technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020.3.E, if the City

Council has not reviewed and approved such item within four City Council meetings from when the item was initially scheduled for City Council consideration, the City shall cease its use of the surveillance technology until such review and approval occurs.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records

City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the City uses the surveillance technology in accordance with its request pursuant to Section 9.64.020.A.1.

9.64.035. Use of Unapproved Technology during Exigent Circumstances or Large-Scale Event

1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a Surveillance Use Policy in two types of circumstances without following the provisions of Section 9.64.030: (A) Exigent circumstances, and (B) a Large-scale event.
2. If City staff acquires or uses a surveillance technology in the two circumstances pursuant to subdivision (1), the City staff shall:
 - A. Use the surveillance technology to solely respond to the Exigent circumstances or Large-scale event.
 - B. Cease using the surveillance technology when the Exigent circumstances or Large scale event ends.
 - C. Only keep and maintain data related to the Exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.
 - D. Following the end of the Exigent circumstances or Large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.
3. Any technology temporarily acquired in Exigent circumstances or during a Large-scale event shall be returned within seven days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If

the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

9.64.040. Oversight Following City Council Approval

1. On March 15th of each year, or at the next closest regularly scheduled Privacy Advisory Commission meeting, City staff must present a written Annual Surveillance Report for Privacy Advisory Commission review for each approved surveillance technology item. If City staff is unable to meet the March 15th deadline, City staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.
 - A. After review by the Privacy Advisory Commission, City staff shall submit the Annual Surveillance Report to the City Council.
 - B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the corresponding Surveillance Use Policy that will resolve the concerns.
 - C. Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the Annual Surveillance Report.
 - D. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 9.64.030 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval.
2. Based upon information provided in City staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory

Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030.2.B and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the City's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

9.64.050. Enforcement

1. Violations of this article are subject to the following remedies:
 - A. Any violation of this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective City department, and the City of Oakland, and, if necessary to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Ordinance, to the extent permitted by law.
 - B. Any person who has been subjected to a surveillance technology in violation of this Ordinance, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in the Superior Court of the State of California against the City of Oakland and shall be entitled to recover actual damages (but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater).
 - C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (A) or (B).
 - D. Violations of this Ordinance by a City employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any Memorandums of Understanding with employee bargaining units.

9.64.060. Secrecy of Surveillance Technology

It shall be unlawful for the City to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the City shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

9.64.070. Whistleblower Protections.

1. Neither the City nor anyone acting on behalf of the City may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:
 - A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or
 - B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Ordinance.
2. It shall be grounds for disciplinary action for a City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any Surveillance Use Policy or Administrative Instruction promulgated under this Ordinance.
3. Any employee or applicant who is injured by a violation of this section may institute a proceeding for monetary damages and injunctive relief against the City in any court of competent jurisdiction.

SECTION 3. Existing Surveillance Use Policies for the Domain Awareness Center, Forward Looking Infrared Thermal Imaging Camera System, and Cell Site Simulator, Must Be Adopted as Ordinances.

Within 180 days of the effective date of this ordinance, City staff shall return to City Council with an ordinance or ordinances adopting and codifying the following surveillance use policies under the Oakland Municipal Code: the Domain Awareness Center (DAC) Policy for Privacy and Data Retention (Resolution No. 85638 C.M.S., passed June 2, 2015); the Forward Looking Infrared Thermal Imaging Camera System (FLIR) Privacy and Data Retention Policy (Resolution No. 85807 C.M.S., passed October 6, 2015); and the Cell Site Simulator Policy (Resolution No. 86585 C.M.S., passed February 7, 2017) .

SECTION 4. Severability. If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional.

SECTION 5. Effective Date. This ordinance shall become effective immediately on final adoption if it receives six or more affirmative votes; otherwise it shall become effective upon the seventh day after final adoption.

IN COUNCIL, OAKLAND, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL-WASHINGTON, GALLO, GIBSON MCELHANEY, GUILLÉN, KALB, KAPLAN
AND PRESIDENT REID

NOES -

ABSENT -

ABSTENTION -

ATTEST: _____
LATONDA SIMMONS
City Clerk and Clerk of the Council
of the City of Oakland, California

Date of Attestation: _____

NOTICE AND DIGEST

ORDINANCE ADDING CHAPTER 9.64 TO THE OAKLAND MUNICIPAL CODE ESTABLISHING RULES FOR THE CITY'S ACQUISITION AND USE OF SURVEILLANCE EQUIPMENT

This ordinance sets rules for how the City of Oakland acquires and uses surveillance technology. It requires the City to establish policies governing the use of surveillance technology. It also provides a review process for new and existing surveillance technology whereby the Privacy Advisory Commission will evaluate and provide a public forum for discussion on proposed and existing City surveillance technology in regards to privacy rights, public safety, and fiscal considerations. The Ordinance also specifies that City Council approval is required for the City to use new and existing surveillance technology. Further, it establishes an ongoing review process for City Council, on an annual basis to evaluate whether already approved surveillance technology should continue to be used based on the same considerations referenced above.



CITY OF SOMERVILLE

ORDINANCE NUMBER 2019-16

IN CITY COUNCIL: June 27, 2019

BAN ON FACIAL RECOGNITION TECHNOLOGY

Be it ordained by the City Council, in session assembled, that Chapter 9 of the Code of Ordinances of the City of Somerville, is hereby amended by adding to the existing Article III a new Section 9-25 as follows.

Section 9-25. Banning the usage of facial recognition surveillance technology.

(a) Definitions.

- (1) *Face surveillance* shall mean an automated or semi-automated process that assists in identifying or verifying an individual, based on the physical characteristics of an individual's face.
- (2) *Face surveillance system* shall mean any computer software or application that performs face surveillance.
- (3) *Somerville* shall mean any department, agency, bureau, and/or subordinate division of the City of Somerville.
- (4) *Somerville official* shall mean any person or entity acting on behalf of the City of Somerville, including any officer, employee, agent, contractor, subcontractor, or vendor.

(b) Ban on Government Use of Face Surveillance.

It shall be unlawful for Somerville or any Somerville official to obtain, retain, access, or use:

- (1) Any face surveillance system; or
- (2) Any information obtained from a face surveillance system.

(c) Enforcement.

- (1) *Suppression*: No data collected or derived from any use of face surveillance in violation of this ordinance and no evidence derived therefrom may be received in evidence in any proceeding in or before any department, officer, agency, regulatory body, legislative committee, or other authority subject to the jurisdiction of the City of Somerville.
- (2) *Cause of Action*: Any violation of this Ordinance constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance. An action instituted under this paragraph shall be brought against the City and, if necessary to effectuate compliance with this Ordinance, any other governmental agency with possession, custody, or control of data subject to this Ordinance.
- (3) The City will address alleged violations of this ordinance in accordance with its usual practices, applicable law and contractual obligations.

-
- (4) Nothing in this section shall be construed to limit any individual's rights under State or Federal law.

Approved:

President, City Council

PROTECTING ★ THE ★ UNPROTECTED

Facial-Recognition Inquiries

A Special Report

Whether accessed by local, state or federal law enforcement, Ohio's facial-recognition database is used only for crime-fighting and is protected by limited access, strict rules and regular oversight.



DAVE YOST
OHIO ATTORNEY GENERAL

Executive Summary

In early July, The Washington Post published a story headlined “FBI, ICE find state driver’s license photos are a gold mine for facial-recognition searches.”

The story asserted that the Federal Bureau of Investigation and Immigration and Customs Enforcement “have turned state driver’s license databases into a facial-recognition gold mine, scanning through millions of Americans’ photos without their knowledge or consent...”

It also asserted that federal agencies have “turned state departments of motor vehicles databases into the bedrock of an unprecedented surveillance infrastructure.”

Although Ohio was not named in the story, the next day The Columbus Dispatch published a story outlining Ohio’s facial-recognition database and noting that it had been used by federal agencies.

Ohio’s facial-recognition database is just one of 22 applications and data sets that are part of an online search system called the Ohio Law Enforcement Gateway, or OHLEG. This is an electronic information network that allows law enforcement agencies and related criminal justice agencies to share criminal justice data efficiently and securely. Its purpose is to help these agencies investigate and prevent crime. It is operated by the Bureau of Criminal Investigation, a division of the Ohio Attorney General’s Office.

Following these newspaper stories, Ohio Attorney General Dave Yost directed his staff to review the state’s facial-recognition system to detail how it is used, what safeguards prevent abuse and who has access to the technology. This report is the result of that review.

Summary of the results of the Ohio Attorney General’s review

The key finding of the review is that federal agency searches of Ohio’s facial-recognition database constitute just 3.8 percent of all facial-recognition searches conducted since 2017. All were conducted in accordance with stringent OHLEG requirements and safeguards limiting searches to legitimate criminal justice purposes. There is no evidence of federal misuse of the facial-recognition database, such as for mass surveillance, broad dragnets or other illegitimate uses.

Other findings of the review include:

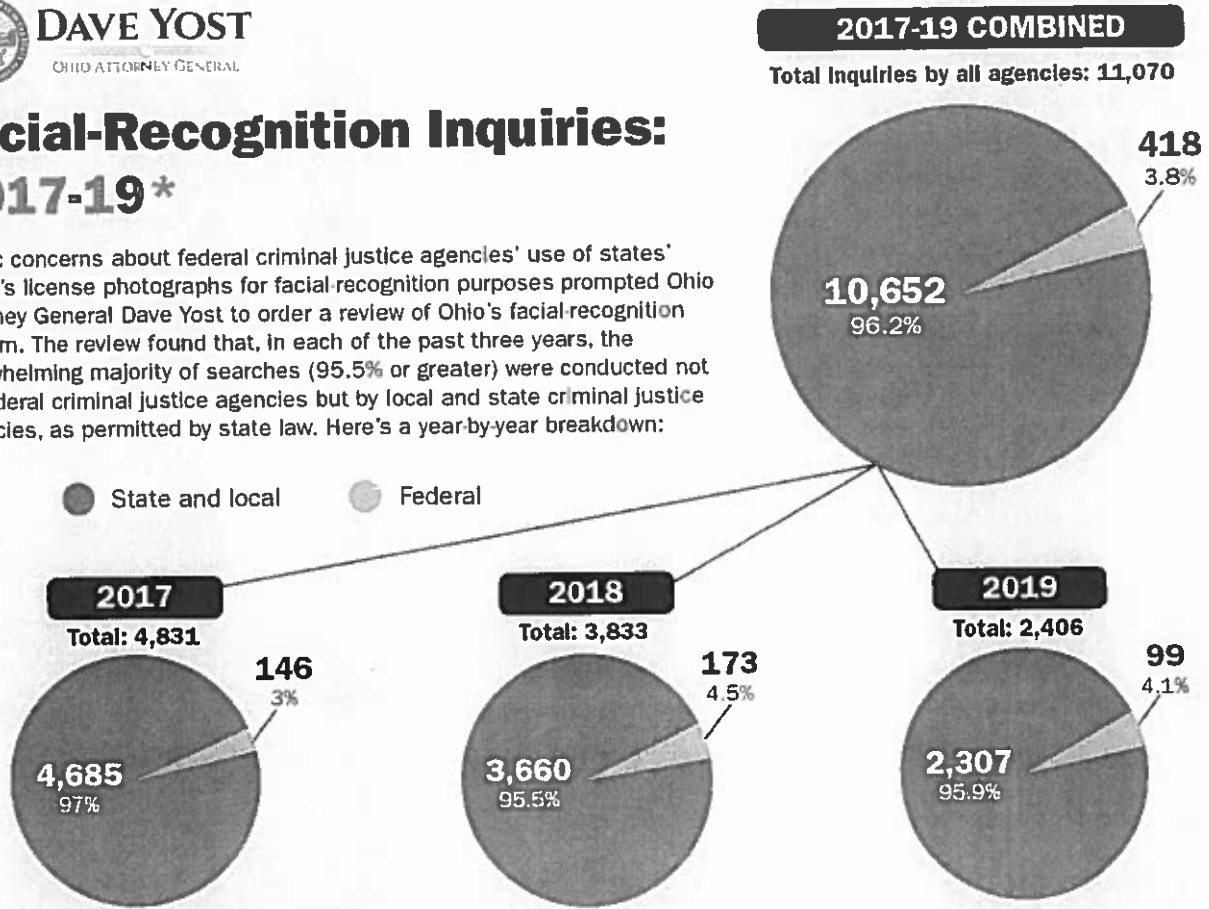
- Ohio’s facial-recognition technology is strictly controlled through OHLEG, which provides criminal justice agencies access to a wide variety of databases containing information vital to the investigation of crime and missing persons. One of those databases is the facial-recognition database.
- OHLEG is used only for criminal justice purposes. Those with access include local and state law enforcement agencies, federal law enforcement agencies, courts, and government agencies that include divisions with investigative powers, such as an inspector general.
- All users of the facial-recognition portion of OHLEG are Ohio-based or, in the case of federal agencies, have offices in Ohio. There are no out-of-state users of the facial-recognition system.
- Access to the facial-recognition database is more restricted than that for other OHLEG databases and is available only to those who demonstrate a specific need.
- Currently, there are 52,680 OHLEG user accounts. However, 15,382 of these accounts have a status of *disabled* because they have not logged in for 120 days. To regain access, these users would have to complete a new application. An additional 11,740 users are *suspended* because they have not logged in for 90 days. To regain access, they would have to contact OHLEG to reset their password. This leaves 25,558 active user accounts, 4,549 of which have facial-recognition access.
- Every user of the facial-recognition system must have an approval from his or her agency head before being assigned a unique log-on, and all searches must be conducted for a legitimate law enforcement purpose under strict guidelines. Each search is recorded for review.
- OHLEG use, including the facial-recognition database, is audited by Ohio Attorney General auditors and by independent outside auditors to ensure that the system is not being abused.
- The OHLEG facial-recognition database contains 24 million images. More than 21 million of these images were supplied

~~by the Ohio Bureau of Criminal Investigation in 2015. It contains 24 million images, with no new images added since 2015.~~



Facial-Recognition Inquiries: 2017-19*

Public concerns about federal criminal justice agencies' use of states' driver's license photographs for facial-recognition purposes prompted Ohio Attorney General Dave Yost to order a review of Ohio's facial-recognition system. The review found that, in each of the past three years, the overwhelming majority of searches (95.5% or greater) were conducted not by federal criminal justice agencies but by local and state criminal justice agencies, as permitted by state law. Here's a year-by-year breakdown:



* 2019 figures reflect database searches through July 31.

From Jan. 1, 2017 until July 31, 2019, Ohio's facial recognition database was accessed for 11,070 searches, including:

2017

- 4,831:** Total inquiries by all agencies
- 4,685:** Total inquiries by state and local agencies (97%)
- 146:** Total inquiries by federal agencies (3%)
- The 146 federal total includes:**
- 59:** Immigration and Customs Enforcement
- 43:** State Department/Bureau of Diplomatic Security
- 37:** FBI Dayton, 32; FBI Cincinnati, 5
- 3:** Bureau of Alcohol, Tobacco and Firearms, Columbus
- 3:** U.S. Marshals Service
- 1:** NASA Glenn Research Center/Office of Protective Services

2018

- 3,833:** Total inquiries by all agencies
- 3,660:** Total inquiries by state and local agencies (95.5%)
- 173:** Total inquiries by federal agencies (4.5%)
- The 173 federal total includes:**
- 97:** U.S. Border Patrol-Sandusky Bay Station
- 32:** State Department/Bureau of Diplomatic Security
- 21:** Immigration and Customs Enforcement
- 6:** FBI Columbus
- 6:** U.S. Marshals Service: Columbus, 3; Akron, 2; Cleveland, 1
- 5:** Drug Enforcement Administration: Toledo, 4; Columbus, 1
- 4:** Federal Reserve Bank of Cleveland
- 2:** Bureau of Alcohol, Tobacco and Firearms, Columbus

2019 (through July 31)

- 2,406:** Total inquiries by all agencies
- 2,307:** Total inquiries by state and local agencies (95.9%)
- 99:** Total inquiries by federal agencies (4.1%)
- The 99 federal total includes:**
- 47:** U.S. Border Patrol, Sandusky Bay Station
- 36:** Immigration and Customs Enforcement
- 15:** State Department/Bureau of Diplomatic Security
- 1:** U.S. Marshals Service

images added since. An additional 2.4 million images were supplied by the Ohio Supreme Court/Ohio Courts Network. The remainder came from various Ohio law enforcement agencies and from the Ohio Department of Rehabilitation and Correction.

- The use of photos from the Ohio Bureau of Motor Vehicles for law enforcement purposes is authorized under state and federal law.
- Federal agencies that have used Ohio's facial-recognition database include the U.S. Border Patrol; U.S. Department of State Bureau of Diplomatic Security; U.S. Immigration and Customs Enforcement; the FBI; Federal Reserve Bank of Cleveland; Drug Enforcement Administration; the U.S. Marshals Service; and the Bureau of Alcohol, Tobacco, Firearms and Explosives; and others.

What is facial-recognition technology?

Facial-recognition technology is software that digitally maps facial features from a photograph or video and uses that data to recognize those same facial features in a different photo or video. With this technology, a photo of an unidentified person can be digitally compared with those in a database of identified images to seek a match.

The accuracy of this technology is rapidly improving, and facial recognition is being applied in a variety of ways. Retailers can use facial recognition to watch for known shoplifters. Similarly, schools could use facial recognition to spot expelled students and other unwanted visitors trying to enter school property.

Apple's latest iPhones use facial recognition to unlock the phones. Social media platforms such as Facebook use facial recognition to identify photos in which Facebook users appear and to help tag them. Airlines have started to use facial recognition to help speed baggage handling, flight check-in and boarding. Such uses are likely to spread, such as for verifying the identity of ATM users.

For law enforcement, facial recognition has a variety of applications. For example, if a video surveillance camera in a bank captures an image of a bank robber, that image can be compared with those in a database of identified images in the hope of finding a match that identifies the perpetrator. The technology also can be used to spot missing persons, abducted children and victims of human trafficking, and to help with cases of identity theft.

Although the technology has many positive uses, it also provokes concerns about privacy and government surveillance. For example, the People's Republic of China is making growing use of facial recognition to monitor members of disfavored ethnic groups and political opponents.

These concerns are legitimate, so it is vital that facial-recognition use by government be conducted only for legitimate purposes and with stringent security to prevent abuse.

Ohio's system comports with state and federal law and has stringent safeguards limiting access and use of all OHLEG data sets, including the facial-recognition database.

OHIO LAW ENFORCEMENT GATEWAY (OHLEG)

Ohio Revised Code Section 109.57(C)(1) provides that the superintendent of BCI may operate a center for electronic, automated, or other data processing for the storage and retrieval of information data and statistics pertaining to criminals and to children under 18 years of age who are adjudicated delinquent children for committing an act that would be a felony or an offense of violence if committed by an adult, criminal activity, crime prevention, law enforcement and criminal justice.

ORC Section 109.57(C)(1) goes on to provide that the superintendent may establish and operate a statewide communications network to be known as the Ohio Law Enforcement Gateway (OHLEG). The purpose of this network is to gather and disseminate information, data, and statistics for the use of law enforcement agencies.

ORC Section 109.57 (C)(5) allows the attorney general to adopt rules under Chapter 119 of the ORC establishing guidelines for the operation of and participation in OHLEG, including criteria for granting and restricting access to information gathered and disseminated through OHLEG. These guidelines have been adopted and are codified in the OHLEG Rules and Regulations. The initial rules were adopted in April 2005, with updates on data security and use policy in June 2014. The rules for facial recognition were adopted in July 2016.

The following rules and regulations apply to criminal justice agencies (CJA) that wish to access OHLEG.

1.0 User Agreement

Any CJA that requests access to OHLEG must sign the OHLEG Agency/User Agreement. The signature of the agency chief executive officer also is required. The agency acknowledges that it is responsible for enforcing and adhering to all OHLEG Security Policies and agrees to accept responsibility for all users from that agency.



Each individual user must sign the OHLEG Agency/User Agreement. All users agree that access to OHLEG is limited to use for criminal justice purposes only.

1.1 Access restrictions

OHLEG law enforcement users are given access to a wider range of OHLEG attributes than are non-law enforcement users, such as court officials. The CEO of each agency is responsible for determining and enforcing access restrictions. Users are permitted to access only those OHLEG attributes that are directly related to their job responsibilities.

Access to individual attributes shall be based on the agency to which the user is assigned at the time of the use. OHLEG users who participate through multiple agencies shall log in to OHLEG using only the OHLEG Agency Identifier number for the agency for which they are working at the time of access. The CEO or designee determines the allowable attributes and should review those determinations when job assignments or responsibilities change. Any law enforcement officer who is a member of a task force may obtain a separate OHLEG account by contacting the OHLEG Support Center.

The nexus between an account holder's job assignment and OHLEG access is subject to review and validation during OHLEG Quality Assurance visits. These reviews are performed by Quality Assurance personnel from BCI, who essentially work as internal auditors. Users shall not attempt to access any data, documents, email correspondence or programs contained on OHLEG information resources for which they do not have authorization.

1.2 Access Control Criteria

Agencies should consider job assignments or functions of the user seeking access; physical location; network addresses; time of day and day of week/month restrictions when establishing rules for access to criminal justice information (CJI).

1.3 System Use Notification

OHLEG will display an approved system use notification message before granting access providing at a minimum the following information:

- The user is accessing a restricted information system.
- Unauthorized use of the system is prohibited and a violation of criminal law.
- System usage is subject to monitoring, recording and auditing.
- Use of the system indicates consent to monitoring and recording – the system includes all data, software, media and hardware.
- The law enforcement data maintained by BCI on the OHLEG site is provided at and subject to the discretion of BCI – BCI's grant of access to OHLEG confers upon the user no process or other rights in maintaining access.

The user must acknowledge the notification message before the user can gain access.

1.4 Personnel Security

Having proper security measures against inside threats is a critical component of the OHLEG security policies. This section's security terms and requirements apply to all personnel who have access to OHLEG, including those individuals with only physical or local access to devices that store, process or transmit unencrypted CJI. Access to OHLEG is a privilege and not a right.

The minimum screening requirements for individuals requiring access to CJI are as follows:

1. To verify identification, state of residence and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to OHLEG or CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to OHLEG.
2. The agency CEO shall specify the agency process for requesting OHLEG access.
3. If a felony conviction of any kind exists, the agency CEO shall deny access to OHLEG. However, the CEO may ask for a review by the OHLEG director in extenuating circumstances in which the severity of the offense and the length of time that has passed might support a variance.
4. If the person has a non-felony conviction or any arrest history without conviction, access to CJI shall not be granted until the agency CEO reviews the matter to determine whether access is appropriate.
5. If the person has an arrest history that includes any theft, domestic violence, menacing or stalking offense; ~~telecommunications harassment; or any misuse of OHLEG, LEADS, or any other restricted law enforcement database or information,~~ the CEO shall deny access. The CEO may ask for a review by the OHLEG director as indicated in #3 above.

6. If the person appears to be a fugitive, the person will be denied access to OHLEG.
7. If the person already has access to CJI and is subsequently arrested and/or convicted of a crime, access to OHLEG shall be terminated. If the crime is a non-felony, OHLEG access may be reinstated following a review by the agency CEO consistent with #4 and #5 above.
8. If the agency CEO, OAC or OHLEG director determines that access to OHLEG by an applicant/user would not be in the public interest, access shall be denied/removed. If access is denied/removed under this section, the agency shall notify the BCI/OHLEG Support Center in writing.
9. BCI/OHLEG's determination as to an OHLEG user's status is independent of, and unrelated to, his/her employment situation with his or her own agency. BCI will not make any determination about an OHLEG user's job status, a matter over which BCI exercises no authority or discretion.

1.5 OHLEG Access Procedure

No OHLEG user shall attempt to gain access to OHLEG or any OHLEG attribute beyond the specific access limits established and authorized by his or her employing agency.

- Requests for OHLEG access will be made via the OHLEG Online Account Application attribute, which is available on the homepage of any current OHLEG user.
- On each new user application, the Approver is required to certify that the basic training security video has been viewed by the applicant and that the OHLEG Agency/User Agreement has been signed by the user.
- The new applicant must physically enter his or her personal information in the appropriate sections on the online application.
- The Approver will select from a checklist the OHLEG attributes approved for each applicant.
- The Approver shall submit applications electronically to OHLEG administration for further processing and activation.
- The facial-recognition attribute will require specific authorization by the CEO of the agency and justification for each user indicating the investigative or other area of responsibility requiring such access.
- Non-law enforcement agencies generally will not have access to the facial-recognition attribute. Any non-law enforcement agency believing it has an exceptional need for access to the facial-recognition attribute may apply to the superintendent of BCI for facial-recognition access.

NOTE – No non-law enforcement agencies currently have, or have had, access to the facial-recognition attribute. A federal agency (which generally refers to law enforcement or criminal justice agencies) may be granted access if it has a presence in Ohio – for example, the FBI has offices in Columbus, Cleveland, Cincinnati and Dayton. On the state level, the BMV has investigators who are considered criminal justice agents.

At one time prior to the administration of Attorney General Yost, out-of-state agents and agencies had access to the facial-recognition database. An Aug. 14, 2014, article in The Cincinnati Enquirer indicates that about 150 users lost access after then-Attorney General Mike DeWine cut off access for out-of-state agencies. No out-of-state agencies currently have access.

Who has access to OHLEG?

The following types of law enforcement agencies have access to OHLEG, though not necessarily access to the facial-recognition attribute:



State

- Police departments
- Sheriff's offices
- Courts
- Parole authorities
- Prosecutors
- City attorneys
- State taxation authorities
- Department of Public Safety investigators
- Ohio State Highway Patrol
- Criminal task forces
- Drug enforcement agencies
- Department of Rehabilitation and Correction
- Ohio Pharmacy Board investigators
- Environmental Protection Agency
- Department of Natural Resources
- Ohio Lottery



Federal

- U.S. Department of Agriculture
- Air Force – Wright-Patterson Air Force Base
- Postal inspectors
- Department of Housing and Urban Development – Cleveland, Cincinnati, Akron
- U.S. Army – Columbus, Cleveland, Youngstown
- U.S. Marshals Service
- U.S. Immigration and Customs Enforcement
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- U.S. Border Patrol – Sandusky Bay
- Coast Guard – Lake Erie
- U.S. Secret Service
- U.S. Department of State
- Treasury Department – Cincinnati
- Department of Labor/Office of Inspector General – Cleveland
- U.S. Attorney's Office – Youngstown, Northern District, Southern District, Southern District of WV
- U.S. Customs – Cleveland
- U.S. Department of Defense Finance and Accounting
- U.S. Department of Education/Office of Inspector General
- Homeland Security
- U.S. Federal Protective Services
- U.S. Fish and Wildlife
- U.S. Forest Service
- Social Security Admin/Office of the Inspector General
Cleveland, Cincinnati

The scope of OHLEG data

OHLEG provides numerous applications and data sets for users:

- OHLEG Online Account Application
- OHLEG Roster (Only the CEO, Application approver or OHLEG Agency Coordinator (OAC) will have access to this application)
- Search Engine (SE) (This is where the facial-recognition attribute is located)
- Search Engine (SE) Admin (OHLEG helpdesk group only)
- Search Engine (SE) Lineup Wizard
- Record Management System
- eOPOTA Learning Management System (LMS) (A redirection to the OPOTA site)
- Missing Children's Clearinghouse
- Laboratory Evidence Pre-log and Inquiry
- Laboratory Online (Prosecutors only)
- OLLEISN Tackle (Ohio Local Law Enforcement Information Sharing Network/ Tracking All Crime Known to Law Enforcement, an information sharing network)
- OPOTA Online Registration and Certification
- Domestic Violence Reports
- Human Trafficking Reports
- Concealed-Carry Permit Statistics
- Pillbox Drug Identification
- Negative DNA Flag Offender Report
- Ohio Protection Order Registry 4.0
- RX Patrol (Provides a link to a nationwide searchable database of prescription-related thefts and related crimes. The database can be used to identify trends, support criminal cases and combat the abuse of prescription drugs.)
- School Safety Plans
- Blue Alerts, Amber Alerts and Missing Adult Alerts
- COLT (New application for sending letters to law enforcement agencies and prosecutors when the Bureau of Criminal Investigation has confirmed a DNA match.)

Audits of OHLEG use

Quality assurance reviews of criminal justice agencies that use OHLEG are conducted every three years by Bureau of Criminal Investigation employees on the OHLEG Quality Assurance Audit Team. In 2018, 135 visits were made to agencies with access to OHLEG.

OHLEG is audited by the following agencies on a triennial cycle:

- National Sex Offender Registry (NSOR)
- Criminal Justice Information Services (CJIS) Security
- Law Enforcement Automated Data System (LEADS),
- National Data Exchange (NDEx)
- National Instant Criminal Background Check System (NICS)
- National Crime Information Center

The facial-recognition database is included in the regularly scheduled audits.

Five cases of OHLEG misuse have been documented in the past two years, but none involved the facial-recognition database. These cases are pending.

Currently, there are 52,680 OHLEG user accounts. However, 15,382 of these accounts have a status of *disabled* because the users have not logged in for 120 days. To regain access, these users would have to complete a new application. An additional 11,740 users are *suspended* because they have not logged in for 90 days. To regain access, they would have to contact OHLEG to reset their password. This leaves 25,558 active user accounts, 4,549 of which have facial-recognition access.

Process for law enforcement to access the facial-recognition system

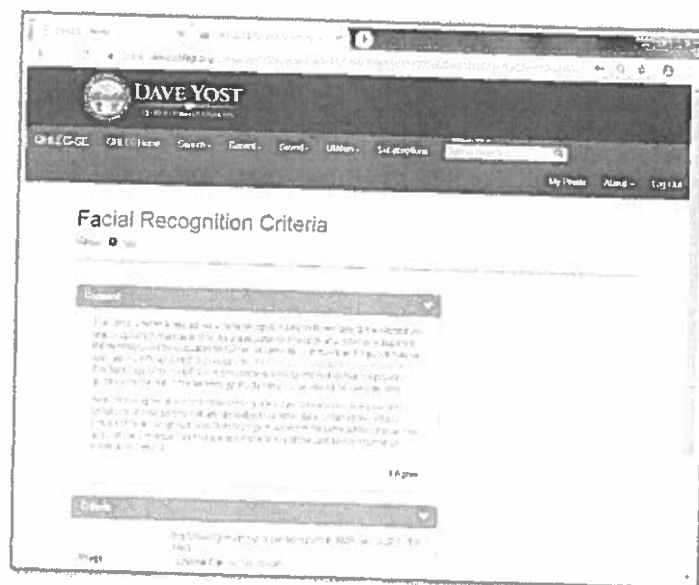
Users of the facial-recognition database are subject to stringent access procedures and auditing practices.

To obtain access to the facial-recognition database:

- An agency must be confirmed to be eligible.
- The agency must be law enforcement (exceptions are permissible, but none has been made).
- The user must submit a new OHLEG application, and the application must be approved by the chief or sheriff of the agency (in limited cases, for very large agencies, there may be an additional facial-recognition approver designated by the chief or sheriff). After the information submitted by the chief or sheriff and the information on the new OHLEG application have been confirmed, the user can be activated for facial-recognition access.

Once the user is authorized to use the facial-recognition attribute, the mechanics for use are as follows:

- The user signs on to OHLEG using his/her personal sign-on information.
- A page appears with the attributes the user has permission to access.
- The user accesses the Search Engine attribute. Once on that page, if the user does not have permission to access facial recognition, it will not be an option on that site.
- When the user accesses the facial-recognition attribute, a consent/waiver appears and the user must agree to terms of use before being able to upload the search photo and launch the application. The consent form reinforces that facial-recognition searches are subject to purpose requirements, limitations and obligations that are applicable to all other data contained on OHLEG.



- The law enforcement officer uploads the search photo and launches the facial-recognition program.
- The application returns photos, and identifiers, of persons matching certain algorithms within the facial-recognition system. The run returns anywhere from zero photos up to 20 photos, depending on the match. As with fingerprints, the better the sample, the greater the likelihood of a useful result.

All facial-recognition search photos submitted by the user and the photos in user-saved search results are stored in the OH-LEG-SE FacialRecognitionImage table with no retention limits. All image keys of facial-recognition search results are stored in the SearchResultFacialRecognition table whether or not the user saves the search results. This allows the user to view recent facial-recognition search results from the Recent Searches menu, even though they may not have saved those results. This also allows the Quality Assurance Audit Team to audit all facial-recognition searches.

Photos in the facial-recognition database

The facial-recognition database consists of photos from a variety of sources.

These photos were sent to a vendor and uploaded into the database. There are currently more than 24 million images in the facial-recognition database (24,380,731 as of July 2019). The sources of those photos include:

- 21,240,729:** Ohio Bureau of Motor Vehicles
- 2,404,041:** Ohio Supreme Court/Ohio Courts Network
- 276,816:** Ohio Department of Rehabilitation and Correction
- 250,056:** Columbus Division of Police
- 174,556:** Hamilton County Sheriff's Office
- 31,351:** Ohio Attorney General's Sex Offender Registry
- 2,173:** Allen County Sheriff's Office
- 385:** Hancock County Sheriff's Office/Findlay Police Department
- 332:** Lima Police Department
- 292:** Jefferson County Sheriff's Office/Steubenville Police Department

Bureau of Motor Vehicle photos

In August 2012, then-BCI Superintendent Thomas Stickrath and Director Thomas Charles, Ohio Department of Public Safety, Bureau of Motor Vehicles entered into a memorandum of understanding under which the BMV would provide information to the AGO and BCI and the BMV could avail itself of the AGO's facial-recognition system and/or receive facial-recognition analytical information from the AGO. The BMV agreed to provide Ohio vehicle registration and driving record information, digitized photographic records of Ohio DL/IDs and other Ohio operator's license information, including demographic information, license number and license status.

The BMV also agreed to transfer to the AGO \$208,500 toward the AGO's development of the facial-recognition system. The AGO agreed to provide the BMV full use of the AGO's facial-recognition system except where use is limited by federal or state law.

The MOU was extended through the years with the most recent extension, Tenth Amendment To and Renewal of the MOU, executed in December 2018 and effective Jan. 1, 2019, through December 2019.

Initially, BMV investigators were using facial recognition to determine if those applying for or renewing an Ohio driver's license were who they said they were. The investigators were able to identify 26 people submitting false identifications between the short time that the facial-recognition program was launched and the temporary suspension of the program by then-Attorney General Mike DeWine for a system review.

Between August and December of 2012, the BMV provided all driver's license ID photos from 2011 and earlier to OHLEG for the facial-recognition database. The BMV has provided no further photos to OHLEG, so all facial-recognition runs are utilizing BMV photos from 2011 and earlier.

State, federal laws governing the use of photos from the Ohio BMV

Ohio Revised Code Section 109.57 sets forth the duties of the superintendent of Bureau of Criminal Investigation. Of note are duties listed in (A)(3) mandating that the superintendent assist sheriffs, chiefs of police and other law enforcement officers in establishing a complete system of criminal identification and in obtaining fingerprints and other means of identification of all persons arrested on a felony charge (and other crimes).

Section (C)(1) authorizes the superintendent to operate a center for electronic, automated or other data for the processing for the storage and retrieval of information, data and statistics pertaining to criminals and delinquents. The superintendent may also establish and operate a statewide communications network (the Ohio Law Enforcement Gateway) to gather and disseminate information, data and statistics for the use of law enforcement agencies and for other uses specified in this division. **Section (C)(3)** allows the superintendent or his designee to provide and exchange the information, data and statistics pursuant to the national crime prevention and privacy compact.

ORC 109.57(C)(5) allows the Ohio attorney general to adopt rules pursuant to Chapter 119 establishing guides for the operation of and participation in OHLEG.

Pursuant to **109.57(D)(4)**, data and statistics gathered or disseminated through OHLEG and other information that is set forth in sections (F) and (G) are not public records.

Although **ORC 4501.27(A)** prohibits the knowing disclosure, or making available, to any person or entity any personal information about an individual that the Ohio BMV obtains in connection with a motor vehicle record, **Section 4501.27(B)(2)** allows for the bureau to disclose such information to a government agency, including a court or law enforcement agency, in carrying out its functions or for the use of a private person or entity acting on behalf of an agency of this state, another state, the United States, or a political subdivision of Ohio or another state in carrying out its function.

Title 18 USC Section 2721 prohibits the release of certain personal information from state motor vehicle records except when there is a permissible use. A permissible use is defined in Subsection (b) and allows for the release in connection with matters of motor vehicle or driver safety and theft. Subsection (b)(1) also allows release of the information for use by any government agency, including any court or law enforcement agency in carrying out its function.

~~While both the federal and state statutes place limitations on the release of personal information from BMV records, they both permit the release of personal information from motor vehicle records to courts and law enforcement agencies carrying out their functions.~~

The proposed memorandum of understanding between BCI, FBI

In August 2017, the FBI and then-BCI Superintendent Thomas Stickrath contemplated entering into an MOU concerning the FBI's use of Ohio's facial-recognition database. This MOU was never executed. It is unclear why the MOU was not executed.

It is worth noting that the proposed MOU would not have given the FBI any elevated access to the database. Essentially, the MOU was intended to ensure that OHLEG's handling of FBI facial-recognition searches was being conducted in compliance with federal regulations governing the confidentiality and use of criminal justice information. However, OHLEG's procedures already are compliant with federal law, making the MOU unnecessary.

Agents from the FBI already were authorized to access the facial-recognition attribute if they were located in Ohio, were authorized to access OHLEG, were approved by the highest ranking agent of their office to access the facial-recognition attribute, approved for access to the facial-recognition attribute and had an active criminal case.

The intent of the proposed MOU was to add layers of protection for the individuals whose pictures were in the database when the facial-recognition attribute was used. The FBI was physically examining the returned photos in an effort to identify only likely candidates. Had BCI and the FBI executed the MOU, the step-by-step process for an FBI special agent to access the database would have been as follows:

- The special agent would send the search photo to the FBI Criminal Justice Information Services Division, or CJIS, in Clarksburg, West Virginia.
- After review by agents at CJIS, the photo would be sent to BCI's Criminal Intelligence Unit (CIU). CIU analysts would upload the photo and run the facial-recognition program. Any results from the search would be sent to agents with the Criminal Justice Information Services Division, who would manually analyze, compare and evaluate the candidate photo gallery against the search photo to determine the most likely candidate.
- The FBI would use the most likely candidate photo in a search of the FBI's Next Generation Identification Interstate Photo System. The results of this search would be compared with and analyzed against the original search photos.
- Once this analysis was completed, the most likely candidate photo would be provided to the requesting FBI personnel as an investigative lead.

Images and information associated with any most likely candidate(s) would be stored in the FBI Case Management System for record keeping, and the other photos and information not associated with a most likely candidate would be destroyed.



DAVE YOST

OHIO ATTORNEY GENERAL

Facial-Recognition Inquiries

For more information about this
report, please contact:

**Ohio Attorney General's Office
30 E. Broad St., 17th Floor
Columbus, OH 43215**

614-466-3840

www.OhioAttorneyGeneral.gov

AUGUST 22, 2019

10 reasons you should be worried about facial recognition technology

by Birgit Schippers, The Conversation

Facial recognition technology is spreading fast. Already widespread in China, software that identifies people by comparing images of their faces against a database of records is now being adopted across much of the rest of the world. It's common among police forces but has also been used at airports, railway stations and shopping centers.

The rapid growth of this technology has triggered a much-needed debate. Activists, politicians, academics and even police forces are expressing serious concerns over the impact facial recognition could have on a political culture based on rights and democracy.

Human rights concerns

As someone who researches the future of human rights, I share these concerns. Here are ten reasons why we should worry about the use of facial recognition technology in public spaces.

(1) It puts us on a path towards automated blanket surveillance

CCTV is already widespread around the world, but for governments to use footage against you they have to find specific clips of you doing something they can claim as evidence. Facial recognition technology brings monitoring to new levels. It enables the automated and indiscriminate live surveillance of people as they go about their daily business, giving authorities the chance to track your every move.

(2) It operates without a clear legal or regulatory framework

Most countries have no specific legislation that regulates the use of facial recognition technology, although some lawmakers are trying to change this. This legal limbo opens the door to abuse, such as obtaining our images without our knowledge or consent and using them in ways we would not approve of.

(3) It violates the principles of necessity and proportionality

A commonly stated human rights principle, recognized by organizations from the UN to the London Policing Ethics Panel, is that surveillance should be necessary and proportionate. This means surveillance should be restricted to the pursuit of serious crime instead of enabling the unjustified interference into our liberty and fundamental

rights. Facial recognition technology is at odds with these principles. It is a technology of control that is symptomatic of the state's mistrust of its citizens.

(4) It violates our right to privacy

The right to privacy matters, even in public spaces. It protects the expression of our identity without uncalled-for intrusion from the state or from private companies. Facial recognition technology's indiscriminate and large-scale recording, storing and analyzing of our images undermines this right because it means we can no longer do anything in public without the state knowing about it.

(5) It has a chilling effect on our democratic political culture

Blanket surveillance can deter individuals from attending public events. It can stifle participation in political protests and campaigns for change. And it can discourage nonconformist behavior. This chilling effect is a serious infringement on the right to freedom of assembly, association, and expression.

(6) It denies citizens the opportunity for consent

There is a lack of detailed and specific information as to how facial recognition is actually used. This means that we are not given the opportunity to consent to the recording, analysing and storing of our images in databases. By denying us the opportunity to consent, we are denied choice and control over the use of our own images.

(7) It is often inaccurate

Facial recognition technology promises accurate identification. But numerous studies have highlighted how the algorithms trained on racially biased data sets misidentify people of color, especially women of color. Such algorithmic bias is particularly worrying if it results in unlawful arrests, or if it leads public agencies and private companies to discriminate against women and people from minority ethnic backgrounds.

(8) It can lead to automation bias

If the people using facial recognition software mistakenly believe that the technology is infallible, it can lead to bad decisions. This "automation bias" must be avoided. Machine-generated outcomes should not determine how state agencies or private corporations treat individuals. Trained human operators must exercise meaningful control and take decisions based in law.

(9) It implies there are secret government watchlists

The databases that contain our facial images should ring alarm bells. They imply that private companies and law enforcement agencies are sharing our images to build watchlists of potential suspects without our knowledge or consent. This is a serious threat to our individual rights and civil liberties. The security of these databases, and their vulnerability to the actions of hackers, is also cause for concern.

(10) It can be used to target already vulnerable groups

Facial recognition technology can be used for blanket surveillance. But it can also be deployed selectively, for example to identify migrants and refugees. The sale of facial recognition software to agencies such as the controversial US Immigration and Customs Enforcement (ICE), which has been heavily criticized for its tactics in dealing with migrants, should worry anyone who cares for human rights. And the use of handheld mobile devices with a facial recognition app by police forces raises the spectre of enhanced racial profiling at the street level.

Debate sorely needed

With so many concerns about facial recognition technology, we desperately need a more prominent conversation on its impact on our rights and civil liberties. Without proper regulation of these systems, we risk creating dystopian police states in what were once free, democratic countries.

<https://techxplore.com/news/2019-08-facial-recognition-technology.html>

2

3

4



27 AUGUST 2019

Halt the use of facial-recognition technology until it is regulated

Until appropriate safeguards are in place, we need a moratorium on biometric technology that identifies individuals, says Kate Crawford.

Kate Crawford

Earlier this month, Ohio became the latest of several state and local governments in the United States to stop law-enforcement officers from using facial-recognition databases. The move followed reports that the Immigration and Customs Enforcement agency had been scanning millions of photos in state driver's licence databases, data that could be used to target and deport undocumented immigrants. Researchers at Georgetown University in Washington DC used public-record requests to reveal this previously secret operation, which was running without the consent of individuals or authorization from state or federal lawmakers.

It is not the only such project. Customs and Border Protection is using something similar at airports, creating a record of every passenger's departure. The technology giant Amazon is building partnerships with more than 200 police departments to promote its Ring home-security cameras across the United States. Amazon gets ongoing access to video footage; police get kickbacks on technology products.

Facial-recognition technology is not ready for this kind of deployment, nor are governments ready to keep it from causing harm. Stronger regulatory safeguards are urgently needed, and so is a wider public debate about the impact it is already having. Comprehensive legislation must guarantee restrictions on its use, as well as transparency, due process and other basic rights. Until those safeguards are in place, we need a moratorium on the use of this technology in public spaces.

There is little evidence that biometric technology can identify suspects quickly or in real time. No peer-reviewed studies have shown convincing data that the technology has sufficient accuracy to meet the US constitutional standards of due process, probable cause and equal protection that are required for searches and arrests.

Even the world's largest corporate supplier of police body cameras — Axon in Scottsdale, Arizona — announced this year that it would not deploy facial-recognition technology in any of its products because it was too unreliable for police work and “could exacerbate existing inequities in policing, for example by penalizing black or LGBTQ communities”. Three cities in the United States have banned the use of facial recognition by law-enforcement agencies, citing bias concerns.

They are right to be worried. These tools generate many of the same biases as human law-enforcement officers, but with the false patina of technical neutrality. The researchers Joy Buolamwin at Massachusetts Institute of Technology in Cambridge and Timnit Gebru, then at Microsoft Research

in New York City, showed that some of the most advanced facial-recognition software failed to accurately identify dark-skinned women 35% of the time, compared to a 1% error rate for white men. Separate work showed that these technologies mismatched 28 US members of Congress to a database of mugshots, with a nearly 40% error rate for members of colour. Researchers at the University of Essex in Colchester, UK, tested a facial-recognition technology used by London's Metropolitan Police, and found it made just 8 correct matches out of a series of 42, an error rate they suspect would not be found lawful in court. Subsequently, a parliamentary committee called for trials of facial-recognition technology to be halted until a legal framework could be established.

But we should not imagine that the most we can hope for is technical parity for the surveillance armoury. Much more than technical improvements are needed. These tools are dangerous when they fail and harmful when they work. We need legal guard rails for all biometric surveillance systems, particularly as they improve in accuracy and invasiveness. Accordingly, the AI Now Institute that I co-founded at New York University has crafted four principles for a protective framework.

First, given the costly errors, discrimination and privacy invasions associated with facial-recognition systems, policymakers should not fund or deploy them until they have been vetted and strong protections have been put in place. That includes prohibiting links between private and government databases.

Second, legislation should require that public agencies rigorously review biometric technologies for bias, privacy and civil-rights concerns, as well as solicit public input before they are used. Agencies that want to deploy these technologies should be required to carry out a formal algorithmic impact assessment (AIA). Modelled after impact-assessment frameworks for human rights, environmental protection and data protection, AIAs help governments to evaluate artificial-intelligence systems and guarantee public input.

Third, governments should require corporations to waive any legal restrictions on researching or overseeing these systems. As we outlined in the AI Now Report 2018, tech companies are currently able to use trade-secrecy laws to shield themselves from public scrutiny. This creates a legal 'black box' that is just as opaque as any algorithmic 'black box', and serves to shut down investigations into the social implications of these systems.

Finally, we need greater whistle-blower protections for technology-company employees to ensure that the three other principles are working. Tech workers themselves have emerged as a powerful force of accountability: for example, whistle-blowers revealed Google's work on a censored search engine in China. Without greater protections, they are in danger of retaliation.

Scholars have been pointing to the technical and social risks of facial recognition for years. Greater accuracy is not the point. We need strong legal safeguards that guarantee civil rights, fairness and accountability. Otherwise, this technology will make all of us less free.

Aug 19, 2019

Facial Recognition Technology: Here Are The Important Pros And Cons **Bernard Marr Contributor**

When you post a photo on Facebook, and the platform automatically tags the people in the image, you might not give much thought to the technology behind the convenience. However, when you discover that facial recognition technology could track you without your permission while you walk down a street in London, it might make you question the invasion of your privacy. Just like with any other new technology, facial recognition brings positives and negatives with it. Since it's here to stay and expanding, it's good to be aware of the pros and cons of facial recognition.

What is facial recognition, and how does it work?

Facial recognition is a biometric technology that uses distinguishable facial features to identify a person. Allied Market Research expects the facial recognition market to grow to \$9.6 billion by 2022. Today, it's used in a variety of ways from allowing you to unlock your phone, go through security at the airport, purchase products at stores and in the case of entertainer and musician Taylor Swift it was used to identify if her known stalkers came through the gate at her Rose Bowl concert in May 2018.

Today, we are inundated with data of all kinds, but the plethora of photo and video data available provides the dataset required to make facial recognition technology work. Facial recognition systems analyze the visual data and millions of images and videos created by high-quality Closed-Circuit Television (CCTV) cameras installed in our cities for security, smartphones, social media, and other online activity. Machine learning and artificial intelligence capabilities in the software map distinguishable facial features mathematically, look for patterns in the visual data, and compare new images and videos to other data stored in facial recognition databases to determine identity.

Pros of facial recognition

One of the major advantages of facial recognition technology is safety and security. Law enforcement agencies use the technology to uncover criminals or to find missing children or seniors. In New York, police were able to apprehend an accused rapist using facial recognition technology within 24 hours of an incident where he threatened a woman with rape at knifepoint. In cities where police don't have time to help fight petty crime, business owners are installing facial-recognition systems to watch people and identify subjects of interest when they come in their stores.

Airports are increasingly adding facial recognition technology to security checkpoints; the U.S. Department of Homeland Security predicts that it will be used on 97 percent of travelers by 2023. When people know they are being watched, they are less likely to commit crimes so the possibility of facial recognition technology being used could deter crime.

Since there is no contact required for facial recognition like there is with fingerprinting or other security measures, facial recognition offers a quick, automatic, and seamless verification experience. There is nothing such as a key or I.D. that can be lost or stolen.

Facial recognition can add conveniences. In addition to helping you tag photos in Facebook or your cloud storage via Apple and Google, you will start to be able to check-out at stores without pulling out money or credit cards—your face will be scanned. At the A.I. Bar, facial recognition technology is used to add patrons who approach the bar to a running queue to get served their drinks more efficiently.

Although possible, it's hard to fool facial recognition technology so it can also help prevent fraud.

Cons of facial recognition

The biggest drawback for facial recognition technology in most people's opinions is the threat to an individual's privacy. In fact, several cities have considered or will ban real-time facial recognition surveillance use by law enforcement, including San Francisco, Cambridge, Massachusetts, and more. These municipalities determined the risks of using the technology outweighed the benefits. Police can still use footage from personally owned devices such as Nest cameras to find criminals; it's just not allowing the government entities to use live facial recognition software.

While London's King's Cross is using facial recognition, London is also at the forefront of democratic societies in its testing of the technology. In test events, the city hopes to determine the accuracy of the systems while grappling with how to deal with individuals who cover up to hide their identity from cameras and other issues. Additionally, democratic societies must define the legal basis to live facial-recognition of the general population, and when blanket use of the technology is justified.

The technology isn't as effective at identifying people of color and women as it is white males. One reason for this is the data set the algorithms are trained on is not as robust for people of color and women. Until this is rectified, there are concerns about the ramifications for misidentifying people with the technology.

In addition, there are issues that need to be resolved that can throw off the technology when a person changes appearance or the camera angle isn't quite right (although they are working on being able to identify a person by only their earlobe). It's dramatically improving; according to independent tests by the U.S. National Institute of Standards and Technology (NIST) facial recognition systems got 20 times better at finding a match in a database over a period that covered 2014 to 2018.

Another potential downside is the storage of sensitive personal data and the challenges that come with it. Just last week, we have had the news that a database containing facial scans used by banks, police forces, and defense firms were breached.

In order to benefit from the positive aspects of facial recognition, our society is going to have to work through some significant challenges to our privacy and civil liberties. Will individuals accept the invasion of their privacy as a proper cost to being more secure and for the conveniences facial recognition provides?

Bernard Marr is an internationally best-selling author, popular keynote speaker, futurist, and a strategic business & technology advisor to governments and companies. He helps organisations improve their business performance, use data more intelligently, and understand the implications of new technologies such as artificial intelligence, big data, blockchains, and the Internet of Things.

<https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/#3ce33c8214d1>

