Initial Report and Recommendations on Cleveland's Emerging Police Surveillance Technology

Cleveland Community Police Commission
Search and Seizure Work Group, Technology Committee
May 9, 2022

Cleveland Community Police Commission

Search and Seizure Work Group, Technology Committee

Committee Chair:

Gordon Friedman, CPC Commissioner

Committee Members *

Jason Goodrick, CPC Executive Director

Ryan Michael Walker, CPC Senior Policy Analyst

Jonathan P Witmer-Rich, Associate Dean, Cleveland-Marshall College of Law

Brian Ray, Director, Center for Cybersecurity and Privacy Protection, Cleveland-Marshall College of Law

Paul Kuzmins, Assistant Public Defender

Lewis Katz, CPC Commissioner, Co-Chair

Gary Daniels, ACLU of Ohio

Leah Winsberg, Children's Law Center

Additional Advisory

Brian Hofer, Executive Director Secure Justice, Oakland, CA

Harold Pretel, Deputy Chief of Homeland and Special Operations, Cleveland Division of Police (CDP)

Kayla Griffin, NAACP Cleveland Chapter

Christopher McNeal, McNeal Legal Services

Cleveland Community Police Commission
www.clecpc.org

*Updated report 5/10/22

The previous version stated the Prosecutor's Office on the list of Committee Members. The Prosecutor's Office did not participate in this report.

Executive Summary

In 2015 the City of Cleveland and the U.S. Department of Justice entered into a Settlement Agreement to reform the Cleveland Division of Police. The agreement, known as a Consent Decree, places heavy emphasis on "trust" and "community input" as pillars of good police policy and decision making going forward. It reads:

> This agreement recognizes the importance of community input into the way police services are delivered. Ongoing community input into the development of reforms, the establishment of police priorities, and mechanisms to promote community confidence in CDP will strengthen CDP and the police community relationship that is necessary to promote public safety…[1] (p. 4) ¶ 14

Further, in regards to the 4th Amendment to the Constitution and the right of privacy from unreasonable Search and Seizure the Decree states:

> CDP will conduct all investigatory stops, searches, and arrests with the goal of ensuring that they are conducted in accordance with the rights secured and protected by the Constitution and state and federal law. CDP will conduct investigatory stops, searches, and arrests fairly and respectfully as part of an effective overall crime prevention strategy that takes into account community values. [2] (p.40) ¶ 160

Over the past several years the Community Police Commission (CPC) has observed an increase in the number of news stories, reports and city council discussions related to use of surveillance technology such as drones, listening devices and smart cameras by the Cleveland Division of Police. Police lawful use of surveillance falls under the umbrella of the 4th Amendment. Based on the Consent Decree and taking into account the history of surveillance technology and how it has been misused by police, particularly against Black citizens advocating for equal civil rights, the CPC took up this important issue.

Following up on an opinion survey in 2021, the CPC formed a committee of experts on police surveillance and privacy law in 2022 to examine best practices for implementing technology into a successful crime prevention strategy, without sacrificing trust or impacting civil liberties. This report serves as the preliminary findings and recommendations of this group.

We have learned that the Cleveland Division of Police, through the Real Time Crime Center, are already using surveillance technology such as Automated License Plate Readers (ALPR), smart cameras that have finite searchable capabilities (possibly utilizing facial recognition), listening devices such as ShotSpotter, and unmanned aerial surveillance systems.

At this stage of our inquiry we have found no evidence that these technologies were implemented in the spirit of the Consent Decree, where the entire community was engaged in evaluating the proposal from the onset and their values were represented. There is also limited or no guidance on their use through General Police Orders (GPOs) which set constitutional policy for officers to ensure this technology is not abused.

[1] US v. Cleveland Consent Decree (2015) p. 4, ¶ 14
justice.gov/sites/default/files/crt/legacy/2015/05/27/cleveland_agreement_5-26-15.pdf
[2] Ibid. p.40, ¶ 160

The CPC understands the importance of creating safe neighborhoods and reducing crime and has no position on the technology itself. However, **how we select, test and utilize new technologies matters**.

Across the U.S. cities that have adhered to a "privacy bill of rights" approach are able to win public support in implementing the technology with proper safeguards in place to build trust. Alternatively, cities that implement new technology in secrecy, without oversight, without policy, and without broad and inclusive public input have found themselves facing scrutiny, lawsuits, and voter referendums to ban certain technologies.

We strongly encourage the City's leadership to consider the following recommendations to increase trust while simultaneously implementing tools to assist in prevention of and solving crime.

Summary of Recommendations

Immediate actions that can be taken:

- CDP should adopt a definition of surveillance technology similar to the City of Oakland, CA:

  > "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, an individual or group."[3]

- CDP should fully disclose to the public its use of any technology that meets this new definition.
- CDP should complete a Surveillance Impact Report for all technology it utilizes that meet the above definition and provide a copy to the Community Police Commission for public dissemination and discussion. *(See Attachment 1)*
- CDP should immediately develop Consent Decree compliant General Police Orders guiding the use of surveillance technologies that it utilizes including but not limited to ShotSpotter, automated license plate readers, drones and smart cameras. The policies should be inclusive of community feedback and community values. *(See Attachment 2)*
- CDP should revise existing Search and Seizure Policy to be more restrictive in regards to technology and privacy including mandating a warrant when an officer wishes to search personal electronic devices, except in exigent circumstances. This is particularly important in relation to interactions with youth.[4]

Long Term Considerations:

The City should establish, through legislation, a broad privacy commission that guides all local government activities in matters of privacy and surveillance technology similar to the City of Oakland model. The privacy commission will work in conjunction with the administration and council to ensure the community is well informed and involved in the adoption of any surveillance technology. The Community Police Commission under Charter Section 115 will be a part of this group when the technology is being utilized for a law enforcement purpose however, in the age of information, government technology and privacy require greater scrutiny then just law enforcement activities. *(See Attachment 3)*

---

[3] Oakland Surveillance and Community Safety Ordinance, 2018, <<eff.org/document/oakland-surveillance-and-community-safety-ordinance-20180426>>

[4] In 2021 the CPC proposed changes to the Search and Seizure GPO that restricted circumstances when officers could search or ask to search the contents of cell phones.

Purpose of Report

The purpose of this report is to propose a new system for the City of Cleveland to assess the adoption of new surveillance technology. The model that the CPC is proposing is based on the City of Oakland, California, widely regarded as the gold standard when it comes to protecting citizens' privacy rights.[5]

The CPC urges Cleveland to formally adopt the City of Oakland's definition of surveillance technology:

> "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, an individual or group."[6]

Emerging technologies reveal the conflict inherent to living in a free society. Citizens have the right to be safe *and* they have the right to privacy. The right to be free from unreasonable search and seizure was codified by the 4th Amendment of the US Constitution. New forms of technology that may allow for the expedient solving of crimes or rendering of aid to those in need can also be used to illegally surveil citizens and violate their constitutional right to privacy. Police have recognized the value of these rapidly growing technologies to listen in to specific conversations on and offline; to observe daily movements of individuals and groups; and to observe data trends.

Surveillance cameras, unmanned aerial drones, and ShotSpotter (an audio system that detects gunshots), are the most commonly discussed emerging police technologies in Cleveland. Other less frequently discussed applications of technology such as facial recognition, automated social media monitoring, DNA databases, biometric data scanning software, stingray technology, GPS tracking, and simply accessing a citizen's cell phone also raise relevant concerns when it comes to ensuring 4th Amendment rights. These new technologies are not flawless crime reduction and investigatory tools. Some of them have come under heavy criticism through academic research including demonstrated biases in software against persons of color and other reliability issues. How we select, test and utilize them matters.

The citizens of Cleveland have valid concerns about these technologies. In the past, Cleveland police officers have abused technology, such as the Law Enforcement Automated Data System (LEADS)[7], to illegally surveil citizens. Nationally, it is well documented that law enforcement has, for generations, used surveillance tools to spy on individuals and groups disproportionately and often illegally. Without local protections in place, Black and brown individuals and members of religious groups have been targeted, often with no consequence to police when discovered.

Cleveland also lags behind other cities, including Oakland, when it comes to instituting protections for citizens' privacy rights. As of now there is no official decision making process regarding the adoption of new surveillance technology, nor are there any known police policies to that effect. The State of Ohio

[5] Nathan Sheard. (2018) "Oakland: The New Gold Standard in Community Control of Police Surveillance," *Electronic Frontier Foundation.*
<<eff.org/deeplinks/2018/05/oakland-new-gold-standard-community-control-police-surveillance>>
[6] Oakland Surveillance and Community Safety Ordinance, 2018,
<<eff.org/document/oakland-surveillance-and-community-safety-ordinance-20180426>>
[7] Henry J. Gomez. (2011) "Cleveland police officer arrested, charged with misusing law enforcement database," *The Plain Dealer/Cleveland.com* <<cleveland.com/metro/2011/07/cleveland_police_officer_arres_1.html>>

also lags behind in protecting citizens' privacy from intrusion of law enforcement as there are no restrictive laws on the books.

To that end the CPC Technology Committee, composed of law professors from Cleveland State and Case Western Reserve, representatives from the ACLU and NAACP, Public Defenders and activists met several times in 2022 to discuss this timely issue and determine a recommended course of local action. The goal: to protect privacy and simultaneously improve public safety.

At the conclusion of these meetings it was proposed that the City of Cleveland adopt a model based on that of the City of Oakland, adjusted as needed, for the particular needs of the Citizens of Cleveland.

Background

On April 28, 2021, the Cleveland City Council Safety Committee met to discuss the adoption of new technology to improve policing in the City of Cleveland. The three newer technologies they were considering were the ongoing ShotSpotter pilot program, the possible use of unmanned aerial drones, and expanding and upgrading the City's surveillance camera system. The committee agreed that these new technologies should be pursued further.

Technologies Under Consideration

Unmanned Aerial Systems (U.A.S. or Drone)

On February 2, 2022, the Committee announced that it was seeking $500,000 for 2 drones, 100 license plate readers, and 5 portable cameras.[8] As of the writing of this report, the City does not have the necessary waivers from the FAA to fly drones from a remote headquarters, as was proposed.

Civil rights advocates, such as the ACLU, have raised concerns that use of these drones could violate citizens' privacy and that there is potential for abuse, similar to past officer abuse of the LEADS System in Cleveland. Some surveillance drones have powerful cameras and microphones which also raises challenging questions in regards to the 4th Amendment limitations on searches. However, if used in a way consistent with the Constitution, research done by Cleveland's Police Inspector General and the CPC suggests that drones could be a promising way to reduce the need for dangerous high-speed police pursuits.[9]

The City of Cleveland Department of Public Safety has publicly stated that their long term goal is to have an unmanned aerial vehicle program similar to Chula Vista, California. Chula Vista has one of the most comprehensive drone operations in the U.S. and utilizes drones as first responders to 9-1-1 calls. Chula Vista emphasizes it has developed a drone program around a set of policies that incorporated

[8] Matthew Richmond. (2022) "Cleveland City Council committee votes to move ahead with license plate reader & drone programs," *Ideastream Public Media* <<ideastream.org/news/cleveland-city-council-committee-votes-to-move-ahead-with-license-plate-reader-drone-programs>>

[9] Cleveland Police Inspector General (2020) "Review and Analysis of Current Division Vehicle Pursuit Policy" <<clevelandohio.gov/sites/default/files/forms_publications/20014-R%20Pursuit%20Compliance%20Memo%206-29-20.pdf>>

community input, public transparency, and respect of privacy. Though being hailed as a model program,[10] there are still concerns expressed by watchdog groups,[11] and Cleveland has none of the prerequisite programs or policy in place to ensure oversight and protection. Chula Vista utilizes impact studies, comprehensive data retention policies, data access policies, and provides transparent tracking data for their drones with an accompanying dashboard showing to which calls drones were deployed.[12]

ShotSpotter

The ShotSpotter pilot program has not yet been renewed, as Council has said it will need more citizen input.[13] The City currently spends $205,000 a year to cover a 3 square mile area in the 4th District around the Mount Pleasant and Buckeye neighborhoods; the program costs $65,000 per square mile with a $10,000 connection fee per year. Cleveland Police claim that the technology saved 6 gunshot victims, due to quicker ambulance response times. Police also claim that the program helped officers seize 34 guns and make 28 arrests.[14]

Nationwide, research suggests that ShotSpotter has a mixed record. The system did not result in across the board reductions in gun violence, and it did not have a significant effect on firearms related arrests.[15] The ACLU[16] and other privacy advocates have suggested that this technology, because microphones are always listening, violate citizens' rights to privacy. In the past, the Shotspotter analysis has resulted in innocent people being arrested and jailed because of flaws in its algorithm.[17]

---

[10] Smart Cities Connect. (2021) "Chula Vista Drone Program Lauded For Accountability, Transparency" <<smartcitiesconnect.org/chula-vista-drone-program-lauded-for-accountability-transparency/>>

[11] Amita Sharma. (2022) "Chula Vista's use of Chinese drones raises alarms," *KPBS* <<kpbs.org/news/local/2022/01/14/chula-vistas-use-of-chinese-drones-raises-red-flags>>

[12] City of Chula Vista. "Drone Program" <<chulavistaca.gov/departments/police-department/programs/uas-drone-program>> Accessed May 2, 2022

[13] Matthew Richmond. (2022) "Cleveland Expands Surveillance Network With ShotSpotter And Private Cameras," *Ideastream Public Media* <<ideastream.org/news/cleveland-expands-surveillance-network-with-shotspotter-and-private-cameras>>

[14] Olivia Mitchell. (2022) "Cleveland police say ShotSpotter is helping to reduce gun violence, but critics question its effectiveness," *The Plain Dealer/Cleveland.com* <<cleveland.com/news/2022/03/cleveland-police-say-shotspotter-is-helping-to-reduce-gun-violence-but-critics-question-its-effectiveness.html>>

[15] Doucette, M.L., Green, C., Necci Dineen, J. et al. Impact of ShotSpotter Technology on Firearm Homicides and Arrests Among Large Metropolitan Counties: a Longitudinal Analysis, 1999–2016. J Urban Health 98, 609–621 (2021). https://doi.org/10.1007/s11524-021-00515-4

[16] Jay Stanley. (2021) "Four Problems with the ShotSpotter Gunshot Detection System," *ACLU* <<aclu.org/news/privacy-technology/four-problems-with-the-shotspotter-gunshot-detection-system>>

[17] Garance Burke, Martha Mendoza, Juliet Linderman, & Michael Tarm. (2022) "How AI-powered tech landed a man in jail with scant evidence," *Associated Press* <<apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220>>

Surveillance Cameras & Facial Recognition

Council has appropriated $4.5 million of the COVID relief money to purchase more city-operated surveillance cameras, of which there are currently 1,200.[8] The City is also looking at other ways to access private cameras with cooperation from citizens and businesses. The City operated cameras run 24/7, but are only monitored by officers for 12 hours a day. Recordings from these cameras and data from license plate readers are kept for 9 months before they are deleted. Footage from these cameras is analyzed at the Real Time Crime Desk by officers and civilian employees.[18]

While there have been license plate readers in Cleveland since 2017, those were operated by Cuyahoga County. This year the City purchased 100 of its own license plate readers that the City will operate.[8] These readers scan every plate that passes by them 24 hours a day. This would give Cleveland Police the ability to track vehicles' movements remotely, passively, and across several months. It can be a powerful tool to track stolen vehicles or vehicles suspected of use in a crime, but it also tracks everyone, all day, every day.

On April 27, 2022, the City updated the Council's Safety Committee on the progress of installing and maintaining City owned surveillance cameras. There was some discussion about the possibility of using these cameras for facial recognition, but the Safety Director recommended that such a conversation be held in private.[19] The use of surveillance cameras has long been a concern of privacy advocates, the possible addition of facial recognition technology is particularly concerning. This technology gives the government the power to track people going about their daily business;[20] facial recognition also has a history of racial bias.[21]

Phone Searches and Social Media

While City Council has not taken up extensive discussion on police engaging in warrantless searches of cell phones and social media monitoring, these are also concerns that the citizens of Cleveland feel need to be addressed. The CPC has, when suggesting changes to the Search and Seizure GPOs, recommended that Cleveland Police officers not search, or ask to search, citizens' cell phones without a warrant, particularly younger citizens.

As the 4th Amendment protects the privacy of one's papers, this protection extends to digital papers as well. In terms of social media monitoring, given the troubled history of Cleveland surveilling activists without warrants,[22] the City should put in place a system where such surveillance is regulated by policy and never conducted without proper warrants.

[18] Cleveland City Council Public Safety Committee Meeting, April 27, 2022 <<youtu.be/cj_yryoz0jw?t=5340>>
[19] Ibid <<youtu.be/cj_yryoz0jw?t=7330>>
[20] Kate Conger, Richard Fausset, & Serge F. Kovaleski. (2019) "San Francisco Bans Facial Recognition Technology," The New York Times <<nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>>
[21] Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. *The Alan Turing Institute*. https://doi.org/10.5281/zenodo.4050457
[22] Brandon E. Patterson. (2016) "Are Police Targeting Black Lives Matter Activists Ahead of the GOP Convention?" *Mother Jones* <<motherjones.com/politics/2016/06/cleveland-protesters-rnc-police-fbi-visits/>>

Importance of Public Input

As previously mentioned, the City of Cleveland is behind other cities in protecting citizens' privacy rights against increasingly sophisticated police technology. It is encouraging that the City wants more citizen input for its ShotSpotter program, but often conversations about citizen privacy and the use of new technology happen behind closed doors.

If the City is discussing the use of facial recognition technology, something often employed in authoritarian governments, the discussion needs to be public. By adopting the Oakland model, outlined below, Cleveland should be able to catch up with cities like Oakland in protecting the privacy rights of its citizens.

Public input is necessary to ensure that the people trust the police with any new technology. Research has shown that the public trust in the police will lead to their support of new police technology. [23]

In April, 2021 the CPC conducted a survey of Cleveland citizens, asking about their thoughts on the new police technology. Findings showed that Citizens of Cleveland are open to the police employing technology in ways that help them, with 103 out of 171 responses expressing a generally positive opinion. However, many citizens expressed concern that the police might abuse the technology.[24] This is an opportunity for the City to build on that openness and improve community-police trust overall.

[23] Ben Bradford, Julia A Yesberg, Jonathan Jackson, Paul Dawson, Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support For Police Use of New Technology, The British Journal of Criminology, Volume 60, Issue 6, November 2020, Pages 1502–1522, https://doi.org/10.1093/bjc/azaa032

[24] Cleveland CPC. (2021) "Memorandum on Police Use of New Technology," <<clecpc.org/wp-content/uploads/CPC-Memo-on-Police-Use-of-New-Technology-April-27-2021.pdf>>

Oakland's Model Guiding the Use of Surveillance Technology

Background

The City of Oakland, California, similar to Cleveland, has experienced a complicated relationship between its citizens and its police force. However, the people of Oakland were able to come together and find a way to manage the adaptation of new technology so that citizens' privacy rights are protected.

In 2013, Oakland, because of security concerns around its port, was offered a city-wide surveillance system from the Department of Homeland Security. Initially Oakland's City Council voted to adopt the system without citizen involvement. This prompted protests among Oakland's citizens who challenged the project as violating their privacy rights to *secrecy, anonymity*, and *autonomy*.

This citizen outrage prompted the City Council to restrict the DHS surveillance system to only the port of Oakland. In doing so, Oakland removed city-wide traffic cameras and ShotSpotter maps from their surveillance system. Oakland also established a *Privacy Advisory Commission* (PAC) to provide advice on the best practices meant to protect citizens' privacy rights concerning the adoption of surveillance and data storage technology.

(See Attachment 3 for more details)

Duties and Structure

The duties of this Privacy Advisory Commission (PAC) include:

- Providing advice and technical assistance to Oakland on the best practices to protect citizens' privacy rights
- Drafting model legislation relevant to privacy and data protection
- Submitting annual reports and recommendations on the use of surveillance equipment and whether new policies regarding privacy should be adopted or amended
- Analyzing legislation at every level relevant to the city's use of technology
- Conducting public hearings, making reports
- Presenting findings and recommendations to the City regarding surveillance technology
- Reviewing and making recommendations to the city concerning the DHS surveillance of the Port

The PAC is made up of 9 volunteer commissioners who are appointed by the Mayor of Oakland and confirmed by the City Council. Members of the commission must include at least one: attorney or scholar familiar with privacy and civil rights laws, a past or present member of law enforcement with experience working with surveillance technology, an auditor or accountant, a technology security professional, and a member of an organization that focuses on government transparency and openness. [25]

[25] Oakland Privacy Advisory Commission Bylaws <<cao-94612.s3.amazonaws.com/documents/Bylaws-for-the-Privacy-Advisory-Commission.pdf>> Accessed May 2, 2022

CPC Recommendations

A Two Step Cleveland Approach for Increased Privacy and Public Safety

The CPC recommends adopting the Oakland model with necessary modifications to adapt it to the needs of the citizens of Cleveland. These modifications include partnering this new Privacy Commission with the newly Chartered Community Police Commission, when dealing with law enforcement related surveillance.

Step One: Immediate Recommendations

- CDP should adopt Oakland's or a similar definition of surveillance technology:

  > "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, an individual or group."

- CDP should fully disclose to the public its use of any technology that meets the definition of a surveillance technology above.
- CDP should complete a Surveillance Impact Report for all technology it utilizes that meet the above definition and provide a copy to the Community Police Commission for public dissemination and discussion. (See Attachment 1)
- CDP should immediately develop Consent Decree compliant General Police Orders guiding the use of surveillance technologies that it utilizes including but not limited to ShotSpotter, automated license plate readers, drones and smart cameras. The policies should be inclusive of community feedback and community values. *(See Attachment 2)*
- CDP should revise existing Search and Seizure Policy to be more restrictive in regards to technology and privacy including mandating a warrant when an officer wishes to search personal electronic devices, except in exigent circumstances. This is particularly important in relation to interactions with youth.

Step Two: Ensuring Lasting Protection Against Unlawful Surveillance

The City of Cleveland should establish, through legislation, a broad privacy commission that guides all local government activities in matters of privacy and surveillance technology similar to the City of Oakland's model.

The privacy commission will work in conjunction with the administration and council to ensure the community is well informed and involved in the adoption of any surveillance technology. The Community Police Commission under Charter Section 115 will be a part of this group when the technology is being utilized for a law enforcement purpose. However this privacy commission's scrutiny of the City of Cleveland's use of technology will extend beyond law enforcement activities.

Duties and Structure of Proposed Privacy Advisory Commission

The proposed Cleveland privacy advisory commission should have the following responsibilities:

1. Provide advice and technical assistance to the City of Cleveland on best practices to protect citizen privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores citizen data.
2. Conduct meetings and use other public forums to collect and receive public input on the above subject matter, with an emphasis on collecting input form marginalized communities including: people of color, young people, economically vulnerable people, people with disabilities, and the formerly incarcerated.
3. Draft for City Council consideration, model legislation relevant to the above subject matter, including a Surveillance Equipment Usage Ordinance.
4. Work with the Community Police Commission to develop policies and best practices related to law enforcement surveillance technology, utilizing, when necessary, the CPC's power to subpoena and directly implement policy within the Cleveland Division of Police.
5. Review and make recommendations to City Council on how best to respond to any proposed changes to the operations of any county, state, or federal program that may involve surveillance technology or collection of citizens' data.
6. Provide analyses to City Council of pending federal, state and local legislation relevant to the City's purchase and/or use of technology that collects, stores, transmits, handles or processes citizen data.
7. Submit annual reports and recommendations to City Council regarding the City's use of surveillance equipment, whether new City surveillance equipment privacy and data retention policies should be developed or such existing policies be amended.
8. Rigorously reviewing the alleged crime prevention 'success' of the technology to provide an unbiased accounting of to what extent it is actually achieving its stated public safety goals.

This proposed privacy advisory commission should be of a size and composition which takes into account Cleveland's needs. Backgrounds to be considered for appointment include:

1. An attorney, legal scholar, or activist with expertise in privacy and civil rights
2. A past or present member of member of law enforcement who has worked with surveillance equipment and other technology that collects or stores citizen data
3. An auditor or certified public accountant
4. A hardware, software, or encryption security professional
5. A member of an organization which focuses on government transparency and openness
6. A person under the age of 30
7. Persons living in areas where the technology is deployed, particularly Cleveland's underserved neighborhoods

Putting this new proposed commission into place will ensure that the voices of the citizens of Cleveland are heard and that any new technology adopted by local government will account for the rights of those citizens.

This new proposed privacy advisory commission will increase the citizen's trust and confidence in the City of Cleveland and the Cleveland Division of Police. It will also make the adoption of new surveillance technologies a consistent, thoughtful, inclusive, and deliberate process.

Report Attachments

Attachment 1
Surveillance Impact Report:
Unmanned Aerial Systems (UAS)
Report by the Oakland Police Department, City of Oakland, CA, issued in 2020

Attachment 2
DEPARTMENTAL GENERAL ORDER
I-25: UNMANNED AERIAL SYSTEM (UAS)
Police order by the Oakland Police Department, City of Oakland, CA

Attachment 3
Oakland's Privacy Advisory Commission
History, and Process
Overview by Brian Hofer
Executive Director, Secure Justice
Chair, City of Oakland's Privacy Advisory Commission

Additional Resources

Making Smart Decisions About Surveillance: A Guide for Community Transparency, Accountability & Oversight
ACLU of California, 2016
www.aclunc.org/publications/making-smart-decisions-about-surveillance-guide-community-transparency-accountability

COMMUNITY CONTROL OVER POLICE SURVEILLANCE (CCOPS) MODEL BILL
ACLU, 2021
www.aclu.org/legal-document/community-control-over-police-surveillance-ccops-model-bill

SURVEILLANCE ORDINANCE FACTS IN CALIFORNIA - AS OF JANUARY 6, 2022
Secure Justice
www.smartcitypdx.com/s/Surveillance-PAC-Ordinances-Fact-Sheet-1-6-22.pdf

A Clear Solution to Police Surveillance Creep: Warrants Needed for Biometric Analysis
Theodore Claypoole, American Bar Association
www.americanbar.org/groups/business_law/publications/blt/2020/08/police-surveillance

ACLU Privacy and Surveillance
www.aclu.org/issues/national-security/privacy-and-surveillance

OAKLAND POLICE DEPARTMENT
Surveillance Impact Report: Unmanned Aerial Systems (UAS)

---

1. Information Describing Unmanned Aerial Systems (UAS) and How They Work

An Unmanned Aerial System (UAS) is an unmanned aircraft of any type that is capable of sustaining directed flight, whether pre-programmed or remotely controlled and all of the supporting or attached components designed for gathering information through imaging, recording, or any other means. Generally, a UAS consists of:

- An unmanned aircraft which consists of the chassis with several propellers for flight, radio frequency and antenna equipment to communicate with a remote-control unit, control propellers and other flight stabilization technology (e.g. accelerometer, a gyroscope), a computer chip for technology control, a camera for recording, and a digital image/video storage system for recording onto a secure digital card (SD card);
- A remote-control unit that communicates with the unmanned aircraft via radio frequency; and
- A battery charging equipment for the aircraft and remote control.

UAS are controlled from a remote-control unit (similar to a tablet computer). Wireless connectivity lets pilots view the UAS and its surroundings from a bird's-eye perspective.

UAS have cameras so the UAS pilot can view the aerial perspective. UAS record image and video data onto a secure digital (SD) memory cards. SD cards can be removed from UAS after flights to input into a computer for evidence.

2. Proposed Purpose

UAS offer to significantly improve the capacity of law enforcement (LE) to provide a variety of foundational police services. This technology has already been used with many law enforcement agencies to save lives and help capture dangerous criminal suspects. UAS can support first responders in

hazardous incidents that would benefit from an aerial perspective. Responding to violent crime in Oakland often requires officers to face risks to their safety – in addition to the clear risks faced by members of the public when violent crime is present. In 2019 Oakland saw 75 homicides, 3,334 aggravated assaults (284 with firearms), 189 rapes, and 2,789 robberies. Technology such as UAS can play a vital role in mitigating these omnipresent dangers, by providing a greater view into the immediate surroundings of crime scenes and active pursuits.

Searches for armed and dangerous suspects are more effective and controlled with UAS support; an armed suspect can be hiding in a tree or on a roof. LE can respond accordingly and more safely when provided with this critical information (see Section #10 below "Alternatives Considered" for more information on how UAS compares to alternatives for situational awareness). More informed responses also lead to less injury and less uses of force.

LE agencies have successfully used UAS to locate missing persons, especially in more remote areas – as well as for rescue missions. UAS is also being used during disasters and during any hazardous material releases. The situational awareness UAS provides has also become an important tool for large events (e.g. sport events, parades, and festivals); the aerial view provides information that would otherwise require a much larger deployment of LE personnel to maintain the same level of public safety support. Additionally, UAS offer LE a more efficient system for documenting vehicular collision as well as crime scenes. Furthermore, smaller UAS can be equipped with a loud speaker to communicate (e.g. hostage situations/providing verbal commands and directions to the subject).

As Bryan Smith, APSA[1] Safety Program Manager explains in "Working Together: Deploying Manned and Unmanned Aircraft Safely and Successfully" in Air Beat[2]-July-August 2019 Issue, "What if we (LE) had the ability to coordinate tasking, splitting the airborne support responsibilities between manned (helicopter) and unmanned crews so one could watch the perimeter while another searches below treetop level in the courtyards and windows and a third went head of the entry team?" In the same AirBeat Issue, Charles L. Werner, Chairman, National Council on Public Safety U.S. explains in "Public Safety Drones: The Past, Present, and Future," "Virginia's public safety UAS team in York County used one of its drones to fly into a hostage situation to determine when police could safely enter." The article also details how the Alameda County Sheriff's Office (ACSO) is using its drones for traffic incidents, tactical operations, and search and rescue.

OPD does have access to ACSO UAS. However, OPD must make a formal request for each use. This approval process takes several hours when situations require immediate action. Circumstances may proceed without any

[1] APSA = Airborne Public Safety Association

[2] The Official Journal of the Airborne Public Safety Association

time for advance planning and conditions may involve individuals believed to be armed and dangerous. OPD can better respond to such dangerous situations where UAS offers useful intelligence and mitigates officer danger – by having a separate UAS program; a standalone OPD UAS program will allow for much quicker deployment options.

3. Locations Where, and Situations in which UAS may be deployed or utilized.

OPD proposes to use UAS as outlined in OPD Department General Order (DGO) I-25 "UNMANNED AERIAL SYSTEM (UAS)," Section III "General Guidelines" A "Authorized Use" only for the following situations:

a. Mass casualty incidents (e.g. large structure fires with numerous casualties, mass shootings involving multiple deaths or injuries);
b. Disaster management;
c. Missing or lost persons;
d. Hazardous material releases;
e. Sideshow events where many vehicles and reckless driving is present;
f. Rescue operations;
g. Special events;
    i. Such as large gatherings of people on city streets, sporting events, or large parades or festivals; (see authorization for "large or special events under Deployment Authorization below);
h. Training;
i. Hazardous situations which present a high risk to officer and/or public safety, limited to:
    i. Barricaded suspects;
    ii. Hostage situations;
    iii. Armed suicidal persons;
    iv. Arrest of armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime";
    v. Scene documentation for evidentiary or investigation value (e.g. crime, collision, or use of force scenes);
    vi. Operational pre-planning (prior planning for services of search and arrest warrants. This is would provide up-to-date intelligence (e.g. terrain, building layout) so that personnel allocate appropriate resources and minimize last minute chance

encounters and uses of force);

vii. Service of high risk search and arrest warrants involving armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime"; and

viii. Exigent circumstances

i. A monitoring commander (Lieutenant or above) may authorize a UAS deployment under exigent circumstances. A report shall be completed and forwarded to the Chief of Police and the OPD UAS Coordinator for all UAS deployments authorized under exigent circumstances, for a full review to determine policy compliance.

Potentially, UAS could be deployed in any location in the City of Oakland where one or more of the above situations occur and where the proper authorizations are provided. Fortunately, several of these situations rarely occur – but some do occur regularly, such as arresting armed/dangerous person, and crime scene documentation. OPD regularly needs to document crime, use of force, and/or vehicular collision scenes for evidentiary and/or investigation value. UAS can greatly aid in this documentary process, to memorialize a scene from an aerial or overview perspective. In 2018, OPD made 8,239 arrests that included either a felony charge, a misdemeanor charge that required an arrest (warrant, domestic violence, firearms violation), or both. In 2018 there were 70 homicides, 2,624 robberies, and 2,338 reported cases of aggravated assault. Additionally, OPD continues to authorize the use of armored vehicles several times each month where officers attempt to safely locate and arrest individuals suspected in homicides and other violent crimes – UAS can provide situational awareness in all of these critical incidents to provide a greater level of safety for officers, as well as for nearby civilians.

4. Privacy Impact

OPD recognizes that the use of UAS raises privacy concerns. UAS are becoming ubiquitous in the United States, and there is a growing concern that people can be surveilled without notice or reason. There is concern that UAS can be utilized to observe people in places, public or private, where there is an expectation of privacy. The level of potential privacy impact depends upon factors such as flight elevation and camera zoom magnitude, as well as where the UAS is flown.

The results of the research study titled, "Mission-based citizen views on UAV usage and privacy: an affective perspective[3]," published in February 2016 found that people's perceptions of how UAS impacts privacy relate to use type. The researchers from College of Aeronautics, Florida Institute of Technology, and the Aeronautical Science at Embry-Riddle Aeronautical University (ERAU), College

[3] https://www.nrcresearchpress.com/doi/abs/10.1139/juvs-2015-0031#.XkHEAWhKiUl

of Aviation UAS Lab found that people tend to be less concerned about police UAS use when the technology is only used for specific uses - "concerns for privacy were less in the condition where the UAV was only used for a specific mission than when it was operated continuously." DGO I-25.III.A "General Guidelines, Authorized Use" explains that OPD personnel can only use UAS for specific missions, detailed above in Section 3 "Locations Where, and Situations in which UAS may be deployed or utilized."

5. Mitigations

OPD's DGO I-25 restricts OPD's use of UAS in several ways to promote greater privacy protections.

OPD will only use UAS for specific missions rather than operating continuously, mitigating concerns raised in the February 2016 study cited above.

DGO I-25.III "General Guidelines," A. Authorized Use" Part 3 lists the only allowable uses of UAS (e.g. mass casualty incidents, Arrest of armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime")). DGO I-25.III.A.4 "Deployment Authorization" articulates that an Incident Commander must approve all uses of UAS. DGO I-25.III.A.4 "Deployment Authorization for Large or Special Events" lists the additional requirements for using UAS during these situations; this additional deployment list is required so that OPD considers the need for situational awareness in the context of not restricting the rights of Oakland residents and visitors to freedom of expression in the public domain.

The Federal Aviation Administration (FAA) sets strict flight regulations for all UAS users, including for law enforcement. The FAA provides two law enforcement options for creating acceptable UAS programs (see Attachment A: "Drones in Public Safety: A Guide to Starting Operations"), under 14 Code of Federal Regulation (CFR) part 107, subpart E, Special Rule for Model Aircraft; the agency can designate individual members to earn FAA drone pilot certificates and fly under the rules for small UAS, or receive a FAA certificate to function as a "public aircraft operator" to self-certify agency drone pilots and drones. Either way, these options allow for OPD to use systems under 55 pounds, for flying at or below 400 feet above ground level . Absent an emergency situation warranting a FAA COA/Part 107 waiver-permitted law enforcement response, law enforcement is also restricted from using UAS to fly over or near the following locations:

- Stadiums and Sporting Events;
- Near Airports; and
- Emergency and Rescue Operations (wildfires and hurricanes).

DGO I-25.III.A."Authorized Use," Part 7 "Privacy Considerations," outlines several other protocols for mitigating against privacy abuse:

- OPD UAS personnel must adhere to FAA altitude guidelines – flying below 400 feet helps to ensure that UAS is not used for surveilling overly large geographic areas; OPD will use UAS to focus specifically on specific areas.
- OPD UAS operators shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g. residence, yard, enclosure, place of worship, medical provider's office).
- Operators and observers shall take reasonable precautions, such as turning imaging devices away, to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

DGO I-25.III.B "Restricted Use" explains that:

- UAS and remote control units shall not transmit any data except to each other.
- Data shall only be recorded onto removable SD cards.
- UAS shall not be used for the following activities:
    - Targeting a person based on their individual characteristics, such as but not limited to race, ethnicity, national origin, religion, disability, gender, clothing, tattoos, and/or sexual orientation when not connected to actual information about specific individuals related to criminal investigations;
    - For the purpose of harassing, intimidating, or discriminating against any individual or group; or
    - To conduct personal business of any type.

The technology itself also provides privacy mitigations through information security. The DJI Matrice 210 and DJI Mavic 2 Enterprise systems both use DJI's "OcuSync 2.0" protocol and are encrypted using the leading AES-256 standard as well as password login protection. DJI[4] uses this encrypted software to turn off the radio transmission to all devices except the paired unit controller. However, there is no guarantee that these drone-to-controller radio transmissions cannot be potentially hacked by bad actors (higher grade military level encryption would be cost-prohibitive for OPD). . DJI has produced a "Commitment to Data Security" document (see ***Attachment B***). The document explains protocols undertaken to ensure that flight data is not transmitted back to DJI or other sources (e.g. storing data on a U.S.-based AWS server). DJI's "Implementing Mitigation Measures Recommended By The DHS" (see ***Attachment C***) recommends mitigations that mirror OPD UAS mitigations:

[4] The lead UAS manufacturer for equipment used by police agencies throughout the U.S.

- Deactivate Internet Connection from Device Used to Operate the UAS
- Take Precautionary Steps Prior to Installing Updated Software or Firmware
- Remove Secure Digital Card from the Main Flight Controller/aircraft
- If SD Card is Required to Fly the Aircraft, Remove All Data from the Card After Every Flight

OPD will also commit to using UAS such as from DJI that do not directly connect to the internet; rather, the controllers will use a separate mobile device for possible remote transmission. The UAS have local data built into the controller firmware for flight control.

6. Data Types and Sources

UAS will record using industry standard file types such as (e.g. jpeg, mov, mp4, wav or RAW). Such files may contain standard color photograph, standard color video, or other imaging technology such as thermal. Although UAS can transmit one-way audio from OPD, the UAS technology available today does not currently record sound[5].

7. Data Security

OPD takes data security seriously and safeguards UAS data by both procedural and technological means. The video recording function of the UAS shall be activated whenever the UAS is deployed. Video data will be recorded onto Secure Digital (SD) Cards. OPD DGO I.25.4.B "Data Retention" states video recording collected by OPD UAS shall be deleted from the device within five (5) days unless:

- The recording is needed for a criminal investigation;
- The recording is related to a City of Oakland Police department administrative investigations (Internal Affairs Investigation).; or
- Retention of data is necessary for another organizational or public need when OPD is requested for outside agency criminal investigations, administrative investigations, and/or aiding in natural disasters; the program coordinator shall develop procedures to ensure that data are retained and purged in accordance with applicable record retention schedules (in accordance with DGO I-25, Section IV, Sub-Section B "Data Retention."). Outside agency assist would only be conducted if it is within OPD policies.

The program coordinator shall develop procedures to ensure that all UAS SD card data intended to be used as evidence are accessed, maintained, stored

[5] Microphones could be installed, but the sound of the propellers would make sound indecipherable in current models available to OPD.

and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements.

Electronic trails, including encryption, authenticity certificates, and date and time stamping shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

OPD's Electronic Services Unit (ESU) shall be responsible for the maintenance and storage of UAS equipment. Members approved to access UAS equipment under these guidelines are permitted to access the data for administrative or criminal investigation purposes.

UAS image and video data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes, using the following procedures:

- The agency first makes a written request for the OPD data that includes:
    - The name of the requesting agency.
    - The name of the individual making the request.
    - The basis of their need for and right to the information.
        - A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.
- The request is reviewed by the Chief of Police, Assistant Chief of Police, or Deputy Chief/ Deputy Director or designee and must be approved before the request is fulfilled.
- The approved request is retained on file, and incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.B.

8. Costs

Costs for a UAS program can vary from thousands to hundreds of thousands and beyond. Different types of systems exist that would support police services, and technology continues to evolve. However, OPD personnel have procured some initial bids to start an OPD UAS program. UAS technology updates at a fast pace and we do not want to commit to a current model. The following costs ($46,800 total), provided here as an example, are based on an actual bid for one large UAS and four smaller UAS for different types of missions:

UAS System	Components	Cost
DJI Matrice 210 V2 (one system) – large drone for standard use	Rugged commercial enterprise drone that carry a payload of 5.07 pounds (enough for the powerful zoom camera and infrared camera). System comes with drone body, landing gear, monitor, propellers, battery packs and chargers, cables.	$9,600
	Powerful Zoom lens Camera: Zenmuse Z30 (30x Optical Zoom)	**$2,999**
	Infrared Camera: DJI Zenmuse FLIR XT2 Dual Sensor 640x512 30Hz 13mm Radiometric	$13,200.00
	Six extra batteries: DJI TB55 Intelligent Flight Battery (Extended); $369 x 6	$2,214
	Matrice 200 Series Case	$739
DJI Mavic 2 (four systems) – smaller drone for lighter use as well as for indoor use	Drone body with protection kit, controller, batteries, battery chargers, propellers, cables, other related accessories such as spotlights and one-way speakers; $2,949 x 4	$11,796
	Additional batteries; $169x24	$4,056
	DJI Smart Controller; $549x4	$2,196
		$46,800

OPD will utilize one-time General Purpose Funds and/or look to grant funding such as from the United States Department of Homeland Security Urban Area Security Initiative (UASI).

9. Third Party Dependence

OPD is currently reliant upon the Alameda County Sheriff's Office (ACSO) when exigent circumstances occur that warrant UAS requests. OPD has requested and received UAS support from ACSO four times in 2019. "Use of Unapproved Surveillance Technology Under Exigent Circumstances – January 28, 2019" (see Attachment B) explains the use of ACSO UAS on January 18, 2019 in connection with an OPD observed murder suspect. "Use of Unapproved Surveillance Technology-December 17, 2019" (see Attachment C) December 17, 2018 explains the use of ACSO UAS on

December 15, 2018 in connection with a residential (home invasion) robbery in progress with a suspected armed suspect.

OPD values its relationship with ACSO and the UAS support provided in 2019; However, OPD now hopes to join the growing list of municipal police agencies developing their own UAS programs. The "Proposed Purpose" Section 2 above explains the benefit and local need for such situational awareness. There are several vendors currently manufacturing law enforcement enterprise quality systems. Section 8 "Cost" above details a possible purchase from DJI – a leading manufacturer. However, OPD will solicit competitive bids and reevaluate vendors when this Surveillance Impact Report and connected DGO I.25 Use Policy are approved by the City Council.

10. Alternatives Considered

OPD could continue the status quo by relying on its partnership with ACSO UAS; however, OPD will be able to more efficiently deploy UASs when needed in priority situations, by having its own UAS program. OPD currently relies on ACSO for UAS access, as noted in Section 2 "Proposed Purpose" above. OPD must make a request to ACSO in each time a situation arises that would benefit from UAS use and meets all requirements outlined in the OPD UAS Policy. These requests can take several hours in which case OPD's ability to respond is greatly diminished. In cases such hostage situations, missing persons, or pursuit of homicide investigation suspects, a two or more-hour request period can lead to negative outcomes.

Helicopters also offer sky-view situational awareness during some of the situations described in the Purpose and Impact sections above, but UAS costs are lower and UAS can be used in more situations. Helicopters cost several million dollars as well as $200-$400 per hour for manned flight. Currently OPD only has one functional helicopter because the high cost to maintain them. There are situations where UAS do not offer an alternative - UAS can never replace the helicopter for missions such as active vehicle pursuits, sustained flight, active observations and communications from the helicopter. UAS can only be compared in terms of some situations where a local above-ground perspective is needed.

The much lower costs of UAS however means that they can potentially be deployed in more situations where the cost of maintaining helicopters is too prohibitive. UAS can also provide utility in ways beyond the capabilities of much more expensive helicopters:

- Support during fire and emergency operations – UAS can be flown in lower elevation positions such as near fires to locate possible trapped people where helicopters cannot fly; infrared cameras on UAS can also be used to identify heat spots for fire department attention.

- Finding suspects – UAS can be used to find dangerous violent crime suspects, by being flown in locations such as to view roof tops, in trees, or between buildings.
- Crime and vehicle collision scene investigation – UAS can be used to collect evidence that may be difficult to reach from the ground; UAS can easily be used to provide maps and 3D images within minutes using 3rd party software specifically designed to produce such maps and 3D images using photographic data captured by the UAS; this data is also valuable during court testimony.

Another alternative to the use of UAS or helicopters would be to deploy many officers to events described in DGO I-25. Section III "General Guidelines" A. "Authorized Use." However, a greater deployment of sworn personnel would at times be less effective; A missing persons' event would require many more officers to provide the same information as UAS. Additionally, the use of UAS can also allow OPD to minimize its physical presence in situations where more officers may actually be perceived as unnecessary and even threatening, during large or special events. Furthermore, large officer deployments can cause a greater use of overtime funding and cause negative impacts to OPD's general fund budget.

11. Track Record of Other Entities

Many cities and counties in California and nationwide have begun to implement UAS programs due to the numerous uses cases for law enforcement. The Alameda County Sheriff's Office (ACSO) and Sacramento County Sheriff's Office have developed programs with several types of UAVs and full time deputy positions, and Stanislaus County is beginning to develop their program. Cities such as Citrus Heights, Fremont, Pittsburg, and Torrance all now have UAS programs as well.

Interviews with Citrus Heights PD, Pittsburg PD and the Sacramento County Sheriff's Office all testify to the high use value of developing a UAS program for law enforcement. These agencies have all used UAS for search and rescue missions, emergency situations (e.g. natural gas explosions and fires), and to search for suspects considered armed and dangerous. UAS are also being used by these agencies on a regular basis to document fatal vehicle collision scenes as well as for gunshot scenes to develop 3D models that provide great value for investigations – such capabilities were only possible prior to UAS technology with much more human staff time as well as expensive 3D camera technology.

Citrus Heights PD reported that initially they experienced community concerns around privacy. However, the department was able to explain their

plan to community groups, to show how the program is used and the safety and privacy mitigations they employ. The department reports that this approach has led to greater community support. Pittsburg PD also reported that their community did not express any privacy concerns about their UAS program - but that they ensured transparency through proactive UAS Program communications.

DEPARTMENTAL GENERAL ORDER

I-25: UNMANNED AERIAL SYSTEM (UAS)

Effective Date:

Coordinator: Electronic Services Unit, Special Operations Division

---

UNMANNED AERIAL SYSTEMS (UAS)

The purpose of this order is to establish Departmental policy and procedures for the use of Unmanned Aerial Systems.

I. VALUE STATEMENT

The purpose of this policy is to establish guidelines for the use of unmanned aerial systems (UAS) and for the storage, retrieval, and dissemination of images and data captured by UAS.

II. DESCRIPTION OF THE TECHNOLOGY

A. UAS Components

An Unmanned Aerial System (UAS) is an unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached components designed for gathering information through imaging, recording or any other means. Generally, a UAS consists of:

- A UAV, composed of:
  - Chassis with several propellers for flight
  - Control propellers and other flight stabilization technology (e.g. accelerometer, a gyroscope),
  - Radio frequency and antenna equipment to communicate with a remote-control unit;
  - A computer chip for technology control;
  - A camera; and
  - A digital image/video storage system for recording onto a

digital data memory card;

- A remote-control unit; and
- Battery charging equipment for the aircraft and remote control.

B. Purpose

UAS have been used to save lives and protect property and can detect possible dangers that cannot otherwise be seen. UAS can support first responders in hazardous incidents that would benefit from an aerial perspective. In addition to hazardous situations, UAS have applications in locating and apprehending subjects, missing persons, and search and rescue operations as well as task(s) that can best be accomplished from the air in an efficient and effective manner. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations.

C. How the System Works

1. The FAA Modernization and Reform Act of 2012 provides for the integration of civil unmanned aircraft systems into national airspace by September 1, 2015.
2. UAS are controlled from a remote-control unit. Drones can be controlled remotely, often from a smartphone or tablet. Wireless connectivity lets pilots view the drone and its surroundings from a birds-eye perspective. Users can also leverage apps to pre-program specific GPS coordinates and create an automated flight path for the drone. Another wirelessly-enabled feature is the ability to track battery charge in real time, an important consideration since drones use smaller batteries to keep their weight low.
3. UAS have cameras so the UAS pilot can view the aerial perspective.
4. UAS use secure digital (SD) memory cards to record image and video data; SD cards can be removed from UAS after flights to input into a computer for evidence.

III. GENERAL GUIDELINES

A. Authorized Use

1. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations. UAS operations should be conducted in accordance with FAA approval.

2. Only authorized operators who have completed the required training shall be permitted to operate the UAS.
3. UAS may only be used for the following specified situations:
    a. Mass casualty incidents (e.g. large structure fires with numerous casualties, mass shootings involving multiple deaths or injuries);
    b. Disaster management;
    c. Missing or lost persons;
    d. Hazardous material releases;
    e. Sideshow events where many vehicles and reckless driving is present;
    f. Rescue operations;
    g. Training;
    h. Hazardous situations which present a high risk to officer and/or public safety, to include:
        i. Barricaded suspects;
        ii. Hostage situations;
        iii. Armed suicidal persons;
        iv. Arrest of armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime");
        v. Scene documentation for evidentiary or investigation value (e.g. crime, collision, or use of force scenes);
        vi. Operational pre-planning (planning (prior planning for services of search and arrest warrants. This is would provide up-to-date intelligence (e.g. terrain, building layout) so that personnel allocate appropriate resources and minimize last minute chance encounters and uses of force); and
        vii. Service of high risk search and arrest warrants involving armed and/or dangerous persons (as defined in OPD DGO J-04 "Pursuit Driving" Appendix A, H "Violent Forcible Crime"; and
        viii. Exigent circumstances
        ix. A monitoring commander (Lieutenant or above) may authorize a UAS deployment under exigent circumstances. A report shall be completed and forwarded to the Chief of Police and the OPD

UAS Coordinator for all UAS deployments authorized under exigent circumstances, for a full review to determine policy compliance.

4. **Deployment Authorization**

   a. Deployment of OPD UAS

      i. Deployment of an OPD UAS shall require the authorization of the incident commander, who shall be of the rank of Lieutenant of Police or above.

      ii. Incident commanders of a lower rank may authorize the use of a UAS during exigent circumstances. In these cases, authorization from a command-level officer shall be sought as soon as is reasonably practical.

5. Deployment Logs

   a. ESU shall record details from each UAS deployment onto a flight log which shall be submitted to ESU, and kept on file for FFA records purposes.

   b. Flight logs will provide all mission deployment details for each flight.

6. Privacy Considerations

   a. Operators and observers shall adhere to FAA altitude regulations.

   b. Operators and observers shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g. residence, yard, enclosure). When the UAS is being flown, operators will take steps to ensure the camera is focused on the areas necessary to the mission and to minimize the inadvertent collection of data about uninvolved persons or places. Operators and observers shall take reasonable precautions, such as turning imaging devices away, to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

B. Restricted Use

1. UAS shall not be equipped with any weapon systems or analytics capable of identifying groups or individuals, including but not limited to facial recognition or gait analysis.

2. UAS and remote control units shall not transmit any data except to each other. Data shall only be recorded onto removable SD cards.

3. UAS shall not be used for the following activities:

    a. For any activity not defined by "Authorized Use" Part 3 above.

    b. Conducting surveillance not related to an authorized operation;

    c. Targeting a person based on their individual characteristics, such as but not limited to race, ethnicity, national origin, religion, disability, gender, clothing, tattoos, and/or sexual orientation when not connected to actual information about specific individuals related to criminal investigations.

    d. For the purpose of harassing, intimidating, or discriminating against any individual or group.

    e. To conduct personal business of any type.

C. Communications

Notifications will be made to the Communications Section for notifying patrol personnel, when UAS operations are authorized by a Commander.

IV. UAS DATA

A. Data Collection

The video recording only function of the UAS shall be activated whenever the UAS is deployed, and deactivated whenever the UAS deployment is completed. The UAS operator will rely on SD Cards for video recordings.

B. Data Retention

Video recording collected by OPD UAS shall be deleted from the device within five (5) days unless:

1. The recording is needed for a criminal investigation;
2. The recording is related to a City of Oakland Police department administrative investigations (Internal Affairs Investigation). ;

The program coordinator shall develop procedures to ensure that data are retained and purged in accordance with applicable record retention schedules

C. Data Access

OPD's Electronic Services Unit (ESU) shall be responsible for the maintenance and storage of UAS equipment. Members approved to access UAS equipment under these guidelines are permitted to only access the data for administrative or criminal investigation purposes.

UAS image and video data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the OPD data that includes:
    a. The name of the requesting agency.
    b. The name of the individual making the request.
    c. The basis of their need for and right to the information.
        i. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. The request is reviewed by the Chief of Police, Assistant Chief of Police, or Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.
3. The approved request is retained on file, and incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.B.

D. Data storage, access, and security

The program coordinator shall develop procedures to ensure that all UAS SD card data intended to be used as evidence are accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence. These procedures include strict adherence to chain of custody requirements.

Electronic trails, including encryption, authenticity certificates, and date and time stamping shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

E. Data Sharing

UAS systems deployed by OPD shall not share any data with any external organizations via integrated technology. The UAS only sends data to the flight controller via encrypted radio signals – there is no internet connection for external data sharing.

F. Public Access

UAS data which is collected and retained under subsection B of this section is considered a "law enforcement investigatory file" pursuant to Government Code § 6254, and shall be exempt from public disclosure. UAS data which is retained pursuant to subsection B shall be available via public records request pursuant to applicable law regarding Public Records Requests as soon as the criminal or administrative investigations has concluded and/or adjudicated.

G. Data Protection and Security

All UAS SD card data will be will be secured in a manner (e.g. lockbox) only accessible to ESU personnel. All evidence from UAS SD cards shall be submitted to the OPD Evidence Unit for safe storage.

V. UAS ADMINISTRATION

A. System Coordinator / Administrator

1. The ESU will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations and best practices. The program coordinator shall be responsible for the following

program administration responsibilities.

2. The ESU Unit Supervisor, or other designated OPD personnel shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers all use of the UAS technology during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

3. **FAA Certificate of Waiver or Authorization (COA)**

   COA (Certificate of Authorization) given by the FAA which grants permission to fly within specific boundaries and perimeters. The UAS Coordinator will maintain current COA's consistent with FAA regulations. The ESU Unit Supervisor, or other designated OPD personnel, shall coordinate the application process and ensure that the COA is current.

4. **Submission and evaluation of requests for UAS use**

   The ESU Unit Supervisor, or other designated OPD personnel, shall develop a uniform protocol for submission and evaluation of requests to deploy a UAS, including urgent requests made during ongoing or emerging incidents.

B. Facilitating law enforcement requests

The ESU Unit Supervisor, or other designated OPD personnel, shall facilitate law enforcement access to images and data captured by UAS as allowable by department policy and/or City of Oakland ordinance.

C. Program improvements

The ESU Unit Supervisor, or other designated OPD personnel, shall recommend and accept program improvement suggestions, particularly those involving safety and information security.

D. Maintenance

The ESU Unit Supervisor, or other designated OPD personnel, shall develop a UAS inspection, maintenance and record-keeping protocol to ensure continuing airworthiness of a UAS, and include this protocol in the UAS procedure manual.

E. Training

The ESU Unit Supervisor, or other designated OPD personnel, shall ensure that all authorized operators and required observers have completed all required FAA and department-approved training in the operation, applicable laws, policies and procedures regarding use of the UAS.

F. Auditing and Oversight

The ESU Unit Supervisor, or other designated OPD personnel, shall develop a protocol for documenting all UAS uses in accordance to this policy with specific regards to safeguarding the privacy rights of the community and include this in the UAS procedure manual and the annual UAS report. The UAS supervisor will develop an electronic record of time, location, equipment, purpose of deployment, and number of UAS personal involved. Whenever a deployment occurs the operator will send notification/submit (either electronically or hard copy) to the UAS Supervisor to include the topics listed above. This protocol will allow the UAS supervisor to have a running log of all deployments and assist in the annual report.

G. Reporting

The ESU Unit Supervisor, or other designated OPD personnel, shall monitor the adherence of personnel to the established procedures and shall provide periodic reports on the program to the Chief of Police.

The ESU Unit Supervisor, or other designated OPD personnel, shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that contains a summary of authorized access and use.

H. Training

The ESU Unit Supervisor, or other designated OPD personnel, shall develop an operational procedure manual governing the deployment and operation of a UAS including, but not limited to, safety oversight, use of visual observers, establishment of lost link procedures and secure communication with air traffic control facilities.

By Order of

Susan E. Manheimer

Chief of Police Date Signed:

December 2021

OAKLAND'S PRIVACY ADVISORY COMMISSION

History, and Process

Brian Hofer

Executive Director, Secure Justice

Chair, City of Oakland's Privacy Advisory Commission

The Opportunity

Oakland contemplated building-out a multi-faceted surveillance apparatus

- In 2013, Oakland was given the opportunity to expand its Port's **Domain Awareness Center**
  - DHS would foot the $10.9M bill to build out a city-wide surveillance apparatus to fight terrorism and improve security
  - City council voted to proceed

Community Response

Community backlash was swift and certain

OAKLAND PRIVACY

.....I'VE BEEN WATCHING YOU WATCHING ME

Prompted Oakland residents to organize, protest, and to publically assert a three-part right to privacy:

1. **Secrecy** - *our ability to keep our opinions known only to those we intend to receive them. Without secrecy, people may not discuss affairs with whom they choose, excluding those with whom they do not wish to converse*;
2. **Anonymity** - *Secrecy about who is sending and receiving an opinion or message*; and
3. **Autonomy** - *Ability to make our own life decisions free from any force that has violated our secrecy or anonymity*.

Oakland's Reaction?

The City Council listened to residents

Resolution No.85638
C.M.S. on June 2, 2015

- Voted to **restrict DAC to a Port-focused operation**, removing citywide traffic cameras and ShotSpotter maps from the system;
- Established an **ad hoc Privacy Advisory Committee** to develop a DAC Privacy and Data Retention Policy; and
- Created a permanent **Privacy Advisory Commission** to provide advice to the City of Oakland on best practices to protect Oaklanders' privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores our data

PAC Motivation:

- Surveillance efforts to be guarded against include not just technology capable of accessing non-public places or information (such as wiretaps), ***but also technology which aggregates publicly available information***, providing the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations.
- The use of surveillance technology may threaten the privacy of all citizens, ***including communities defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.***

Volunteer commissioners from each city council district:

- District 1 — Reem Suleiman
- District 2 — Chloe Brown
- District 3 — Brian Hofer (Chair)
- District 4 — Lou Katz
- District 5 — Omar De La Cruz
- District 6 — Gina Tomlinson
- District 7 — Robert T. Oliver
- At Large — Henry Gage III (Co-Chair)
- Mayoral — Heather Patterson

Privacy Advisory Commission

Duties of the Commission

Resolution No.85638
C.M.S. on June 2, 2015

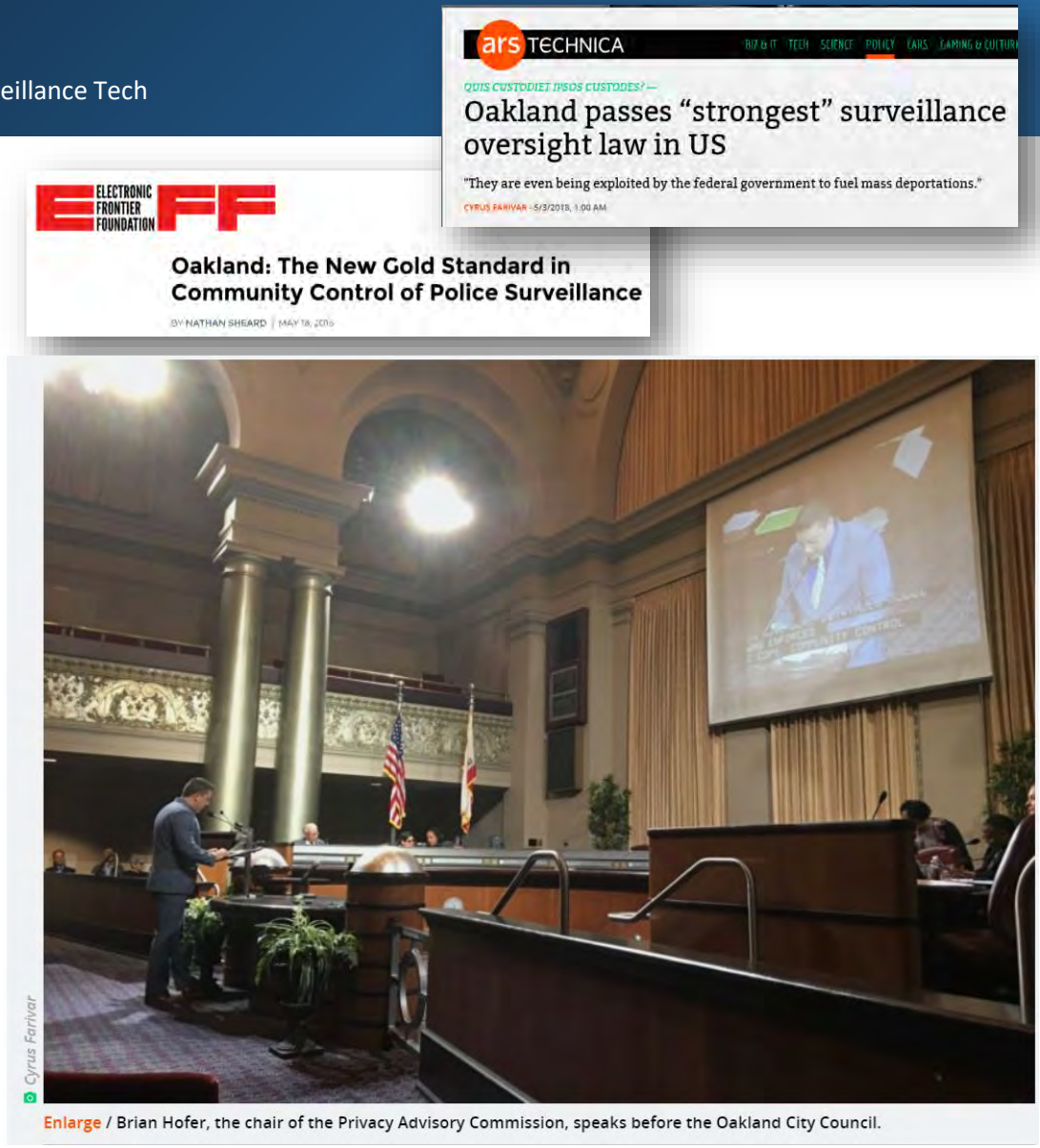
1. **Provide advice and technical assistance** to the City of Oakland on best practices to protect citizen privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores citizen data.
2. **Draft for City Council consideration, model legislation relevant to privacy and data protection**, including a Surveillance Equipment Usage Ordinance.
3. **Submit annual reports and recommendations to the City Council** regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed or such existing policies be amended.
4. **Provide analyses to the City Council of pending federal, state and local legislation** relevant to the City's purchase and/or use of technology that collects, stores, transmits, handles or processes citizen data.
5. **Conduct public hearings, make reports, findings and recommendations** either to the City Administrator or the City Council as appropriate, including an annual report to be presented in writing to the City Council.
6. **Review and make recommendations to the City Council regarding any proposed changes to the operations of the Domain Awareness Center ("DAC")** and/or proposed changes to the City's Policy for Privacy and Data Retention for the Port Domain Awareness Center ("DAC Policy").

Surveillance and Community Safety Ordinance

"Surveillance Ordinance" passed May 2018

Ordinance adding Ch. 9.64 to the Municipal Code Establishing Rules For the City's Acquisition and Use of Surveillance Tech

- **Purpose:** Establish a public approval process for surveillance technologies used by the city; lay the groundwork for the City Council to decide whether the benefits of using the technology outweigh the costs to privacy.
- **City obligations:** City agencies must submit **a "technology impact report"** and a **use policy** to Oakland's Privacy Advisory Commission if they plan to implement new surveillance technologies, like license plate readers or cellphone trackers.
- **"Surveillance Technologies":** 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.
- **Differentiated from other cities**: 1) Standardized public format for evaluation and approval; 2) Prohibits secret contracts or non-disclosure agreements between cities and third parties; 3) Provides whistleblower protections to employees who report violations.



How does the Surveillance Ordinance work in practice? Process for city to acquire or use a surveillance technology

Notification

- City entity **notifies** PAC Chair of its wish to acquire new surveillance technology.

Report Submission

- City entity submits a **Surveillance Impact Report** and proposed **Surveillance Use Policy** to the Privacy Advisory Commission for its review at a regularly noticed meeting.

PAC Evaluation

- PAC reviews documentation, works with City entity to revise Impact Report and Use Policy
- Recommends that the City Council **adopt**, **modify**, or **reject** the proposed Surveillance Use Policy.

Public Notice

- City Council provides **public notice** that will include the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least fifteen (15) days prior to the public hearing.

Public Hearing

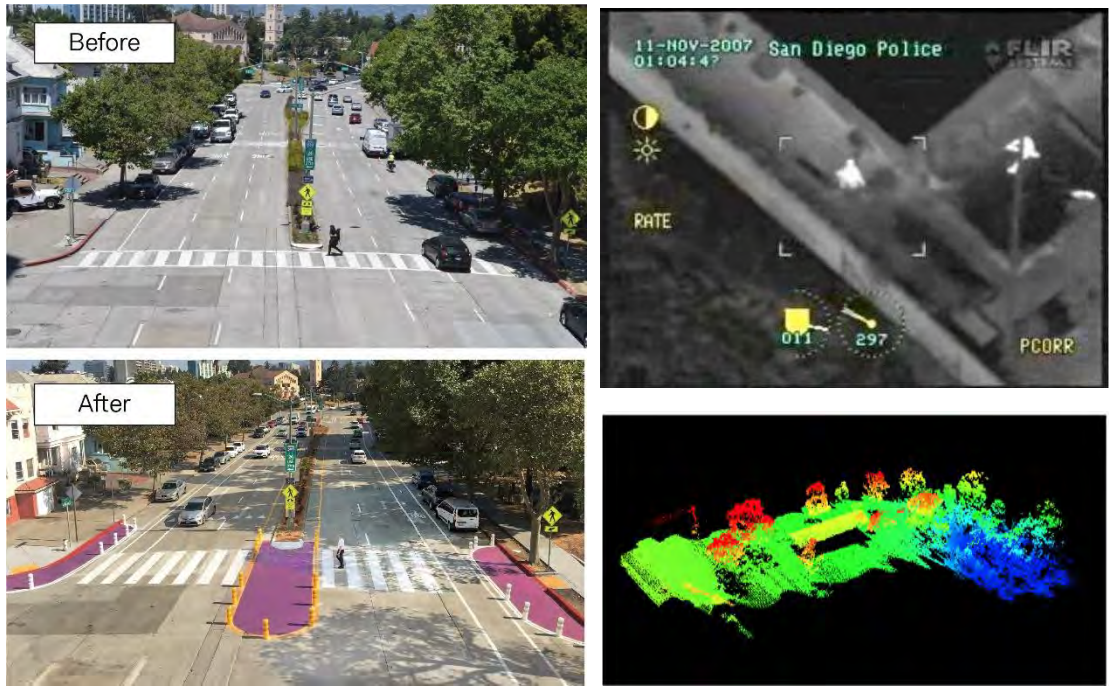
- City Council determination: 1) benefits to the community outweighs the costs; 2) proposal will safeguard civil liberties and civil rights; and 3) no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

Illustrative Examples

Types of requests include:

- DOT acquisition of **Unmanned Arial Vehicles (UAVs)** to document transportation improvement projects;
- DOT Parking and Mobility using vehicle-mounted **Automatic License Plate Recognition (ALPR)** to "virtually chalk" vehicles in time-limited spaces, verify permit parking, monitor "pay by phone" parking payments;
- District Attorney' use of **surveillance video** to monitor illegal dumping;
- Police Dept. use of **cell site simulators** to locate missing persons and apprehend fugitives;
- . . .

E.g., Pending DOT request:



- **Data types and sources:** Optical cameras, IR cameras, LIDAR, mapping software
- **Potential impacts:** Capturing PII without notice or consent; Enabling targeted voyeurism; Data use and retention uncertainties
- **Mitigations:** Deploy only in public and with notice where possible; obfuscate faces and license plates. Two-person team; focus must remain on project

Elements of the Required Documents

(Heart of the ordinance)

Surveillance Impact Report:

A. Description of the technology
B. Proposed use(s)
C. Location to be deployed
D. Impact on civil rights and liberties
E. Mitigations
F. Data types and sources
G. Data security
H. Fiscal cost(s)
I. Third-party dependence
J. Alternative methods
K. Track record

Surveillance Use Policy:

A. Purpose of the use
B. Authorized use(s)
C. Data collection
D. Data access
E. Data protection
F. Data retention
G. Public access
H. Third party data sharing
I. Training
J. Auditing and Oversight
K. Maintenance

Elements of the Required Documents

(Heart of the ordinance)

Annual Report:

A. Summarize how tech was used
B. Data shared with third parties
C. Describe deployment practices
D. Breakdown geographic deployment
E. Summary of community complaints
F. Results of internal audits
G. Information about any data breaches
H. Efficacy
I. Summarize public record requests
J. Total Annual Costs
K. Suggested Policy Amendments

It is important for law enforcement to understand that this is a summary – there is no expectation that raw data will be provided here, nor is there an obligation to provide information so specific as to interfere with active investigations or deployment practices.

Not all categories will be applicable to all surveillance technologies.

The annual review will ideally confirm that the stated goals (provided during the up-front vetting stage) were achieved, whether policy amendments are needed to better achieve those goals, or whether use should discontinue because the technology was either ineffective at achieving its stated goal or was too intrusive and ripe for abuse.

Researching City-wide Privacy Principles

- Design And Use Equitable Privacy Practices
- Limit Collection And Retention Of Personal Information
- Manage Personal Information With Diligence
- Extend Privacy Protections To Our Relations With 3rd Parties
- Safeguard Individual Privacy In Public Records Disclosures
- Be Transparent And Open
- Be Accountable to Residents

How We're Addressing These Challenges

Communicating with technology companies to assess opportunities for protecting privacy

A variety of interesting solutions, depending on use case:

- Data de-identification
- Differential privacy
- Selective sharing of data across silos while assuring confidentiality and privacy
- Tools to enable data obfuscation

Pictures Collected by an AI system before and after applying facial blur policies

Questions?
Interested in engaging?

Please reach out!
We'd love to
hear from you.

brian@secure-justice.org

@b_haddy

@SecureJustice

SECURE JUSTICE