Surveillance and Data Retention Policy Guiding Principles Working Document

Purpose of this Document

The purpose of this working document is to provide an outline and examples of the types of guiding principles which the Council could establish to guide the creation of internal policies for the use of surveillance technology and the retention of surveillance data. Council has provided an initial set of sample guiding principles for staff to review and what follows in this document are comments from both the City Attorney's Office as well as how these principles would apply to the UAS program where applicable.

Example Vision Statement

Council seeks to provide guidelines for the use of surveillance technology to help provide safety and security in the Hayward community with the goal of balancing safety concerns with the co-equal priority of protecting the privacy of our residents.

Example Guiding Principles

A. Data Collection

1. Collection of surveillance data should be restricted to public spaces, unless a warrant is secured or in an emergency.

City Council Comment Summary: The word "emergency" is broad. Can it be removed or better defined?

CAO Response: While the City understands the desire to remove language from the policy allowing the use of drones without a warrant in "emergency" situations, the City is unable to remove that language since federal constitutional law, which the City of Hayward is bound by (preempts state/local law), provides law enforcement with the ability to conduct searches and seizures without a warrant if the search or seizure is conducted:

(1) as to something that is in "plain sight" or in an "open field," meaning it can be seen with the naked eye from an officer lawfully in a position to see it;

(2) incident to the existence of exigent (or emergency) circumstances (also knowns as the community care doctrine in California), meaning officers can enter or search without a warrant to prevent harm to a person, to halt the imminent destruction of evidence, to pursue a fleeing suspect (hot pursuit);

(3) consent is provided; or

(4) incident to an arrest.

These laws would apply to the use of drones/surveillance technology by law enforcement. That said, the use of surveillance technology by law enforcement is already regulated by numerous federal and state laws and regulations, which continue to develop as time goes on and the use of drones becomes more prevalent. See below.

2. Use of surveillance equipment in public, commercial areas is generally permitted.

3. Use of surveillance equipment in residential neighborhoods should generally be avoided, unless an urgent need exists or the neighborhood requests it.

CAO Response: There is an expectation of privacy in both commercial and residential areas, which individuals are entitled to rely on, and which would also apply to law enforcement use of drones and other surveillance technology. In using drones, the Hayward Police Department would be bound by all laws and regulations already governing the use of drones, which includes state and federal regulations and laws. Notably, if state laws or regulations contradict federal laws or regulations, the federal law will likely be the law that is followed. Below is a summary of just some of the laws protecting citizens against the unlawful use of drones/surveillance technology.

A. Laws Regulating Airspace

1. The Air Commerce Act of 1926/ Civil Aeronautics Act of 1938: Generally, the U.S. Federal government has sovereignty over airspace in the U.S. The Acts, authorize the use of technology to fly "within navigable airspace," or airspace "above minimum altitudes of flight prescribed under [49 U.S.C. § 40102(32) and subpart III of that part,] including airspace needed to ensure safety in the takeoff and landing of aircraft.

2. Federal Aviation Association: The FAA has regulated the use of airspace since 1958. The FAA used to regulate all airspace, from the ground up. However, in the ***U.S. v. Causby*, 328 U.S. 256 (1946)** the Supreme Court held that landowners have a right to prevent "intrusions of airspace" and that a landowner owned, "at least as much of the space above the ground as he can occupy or use in connection with the land." Such was interpreted to be the space between the ground and the top of the house or property line. However, the Supreme Court, in that case, also held that navigable airspace, which is a public domain, is "airspace above the minimum safe altitudes of flight," which is 500 feet during the day and 1000 feet at night. Following this case, the FAA controlled airspace was determined to be anywhere over 500 feet. However, since the introduction of drones, the FAA has argued that it has the authority to regulate under 500 feet since the FAA's official policy is that it has sole jurisdiction over all "navigable" or otherwise, airspace.

3. The Modernization and Reform Act of 2012: tasked the FAA with integrating drones into the national airspace system

B. California Civil Laws/Regulations

1. **California Civil Code § 1708.8**: Trespass: provides, "A person is liable for physical invasion of privacy when the person knowingly enters onto the land or into the airspace above the land of another person without permission or otherwise commits a trespass in order to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or familial activity and the invasion occurs in a manner that is offensive to a reasonable person."

2. Private Nuisance. (Civil Code section 3481): A cause of action for private nuisance may arise against unwanted drone usage. The nuisance in this case, is the noise of the drone – the whirring of the engine or blades – disrupting the quiet use and enjoyment of your premises.

3. Injunction. (Code of Civil Procedure section 525-526): An injunction is a writ or order requiring a person to refrain from a particular act.

4. Temporary Restraining Order prohibiting Harassment. (Code of Civil Procedure section 527.6 (a)(1)): A person who has suffered harassment as defined in subdivision (b) may seek a temporary restraining order and an injunction prohibiting harassment.

C. California Criminal Laws

1. Penal Code § 632: Eavesdropping (Invasion of Privacy). While this section discusses eavesdropping or recording of confidential communications by "electronic amplifying or recording device," such would apply to drones to the extent drones use such eavesdropping devices in non-public places, without a warrant or exigent circumstances.

2. Penal Code § 633.8: Police may use electronic amplifying or recording devices to eavesdrop when responding to "an emergency situation that involves the taking of a hostage or the barricading of a location," if the following conditions are satisfied: (1) the officer reasonably determines that an emergency situation exists involving the immediate danger of death or serious physical injury; (2) the officer reasonably determines that the emergency situation requires eavesdropping, immediately; (3) there are grounds upon which an order could be obtained pursuant to Section 2516(d) of Title 18 of the U.S. Code.

3. Penal Code § 634: Trespass (Invasion of Privacy). A person trespasses on property if it is done for the specific purpose of attempting or committing an act of Penal Code section 632. It is possible that police use of a drone over private property will constitute a trespass, if done without a warrant or exigent circumstances.

4. California Assembly Bill No. 1129 (approved by Governor on Oct. 11, 2019): Makes it a misdemeanor offense to operate a drone for the purpose of invading the privacy of a person inside their home or any other interior area where there is a reasonable expectation of privacy.

The purpose of this bill was to extend the privacy protections already given to physical intrusions (looking through a hole into somebody else's house, using a telescope to see into someone's house or a camera) to "electronic devises and unmanned aircrafts" also known as drones.

C. Federal Case Law

1. *Katz v. U.S.*, 389 U.S. 347 (1967): In this case, the Supreme Court held that the Fourth Amendment does not just protect citizens from physical invasions of privacy, but also protects against non-physical intrusions. The case also establishes the expectation of privacy test, to determine whether an individual even has an expectation of privacy in a particular situation. The test requires that two questions be asked:

(1) Did the person intruded upon actually believe they had an "expectation of privacy"; and

(2) is society ready to accept that expectation of privacy as reasonable?

In *Katz,* for instance, the Court held that it was unlawful for police to place a listening device on a public telephone booth without a warrant or exigent circumstances. The Supreme Court reasoned that, although the booth was located in a public thoroughfare, a person enters a phone both in order to keep conversations private, therefore indicating that the person using the phone both had an actual expectation of privacy. The Supreme Court further found that society created phone booths for the exact purpose of keeping phone conversations private. As such, the Court found that law enforcement use of the listening device violated Katz Fourth Amendment rights.

2. *California v. Ciraolo*, 476 U.S. 207 (1986): In this matter, officers had received a tip that marijuana was being grown in a residential backyard. Officers could not see into the backyard since a fence was blocking their view, so they used airplanes to fly overhead and surveil the property. The Supreme Court held that because the airplane flew at an altitude of 1000 feet, as permitted by the Federal Aviation Administration (FAA) regulations, that the residential backyard was thus in "public view" and the resident had no expectation of privacy in his backyard, from the altitude of 1000 feet.

This case establishes two things: (1) That the Supreme Court's decisions will be affected by Federal Aviation Administration regulations, meaning law enforcement agencies are bound not just by case law but by the Federal Aviation Administrative regulations when using flying technology to surveil; and (2) that if a flying surveillance technology is at a certain height above residential property, which is not covered on all four sides, that there may not be an expectation of privacy if surveillance is done from a far enough distance away.

3. *Dow Chemical v. United States,* 476 U.S. 227 (1986): The Environmental Protection Agency requested to take pictures of the Dow Chemical plant. After Dow refused to allow the "search", the EPA simply hired an aerial photographer to take pictures of the plant. Dow filed suit and

ultimately, the Supreme Court held that "the open areas of an industrial plant complex" are not analogous to the 'curtilage' of a dwelling for purposes of aerial surveillance. The Court therefore found that the use of an airplane to take photographs of the industrial plant was not a search under the Fourth Amendment.

The importance of this case is the distinction the Supreme Court makes between residential and commercial property. The Supreme Court indicates, in this case, that the areas outside of a commercial establishment, which may still be considered a part of the establishment, are not analogous to areas just outside of a residential property, such as a porch, patio, backyard or front lawn (curtilage). Thus, although persons have an expectation of privacy in the areas just outside of their home (curtilage), persons do not have such an expectation of privacy in the areas just outside of a commercial property, which may be visible to the public.

4. *Florida v. Riley*, 488 U.S. 445 (1989): The Supreme Court ruled that law enforcement officers flying within the "navigable airspace" allowed under the Federal Aviation Administration regulations, did not violate the Fourth Amendment even though the helicopter was used to view marijuana plants grown in a greenhouse near a mobile home.

5. ***Kyllo v. United States*, 533 U.S. 27 (2001):** In this matter, the police had used a thermal imaging device to detect marijuana being grown inside of a home. The Supreme Court held that the use of the thermal imaging device for surveillance inside of a home constituted an unlawful search under the Fourth Amendment. The Supreme Court reasoned that because the police used a device "not in general public use" to explore "details" of a home that would previously have been unknowable without physical intrusion, that the surveillance is a search that is presumptively unreasonable.

This case is important as it established an added factor to the Supreme Court's analysis of whether an action constitutes a search: whether or not the device used to conduct the search was "in general public use," and thus even contemplated by the person who expected to have such privacy. This may become more relevant in the context of drone cases, as the technology and its abilities are still new.

6. ***United States v. Jones*, 565 U.S. 400 (2012):** In this more recent case, the U.S. Supreme Court held that a law enforcement agency's action of placing a GPS device onto a car without a warrant or exigent circumstances, not only constituted a violation of the fourth Amendment, but also a trespass into a constitutionally protected area. In comparing this case to the other Supreme Court cases regarding the use of surveillance technology, it appears the Supreme Court is making a distinction between surveillance devices which require physical attachment to personal property, versus the use of aerial surveillance at a certain height to view such property.

This is not an exhaustive list of the laws and regulations which law enforcement agencies must abide by when using surveillance technology, such as drones, and case law is constantly creating more tests and regulations as further lawsuits are brought.

UAS Application Response:

The use of the drone is addressed in the proposed Police Department Unmanned Aerial System (UAS) Operations Policy and includes public safety and life preservation missions. Further detail may be found in the policy under the USE OF UAS section.

B. Data Storage and Retention

1. Storage of surveillance data should be on secure servers where access is restricted to law enforcement personnel. Data access by authorized personnel should be tracked and logged.

Proposed change: Add language which includes that vendors should adhere to CJIS guidelines and obtain CJIS certification which addresses data access, storage, and auditing.

City Council Comment Summary: If events are logged, then they should include an audit trail. In addition, data should be stored on servers located in the US and adhere to US government standards.

UAS Application Response:

Data from this program will be stored in Evidence.com which is a CJIS certified cloud-hosted system. CJIS Policy Area 4: Auditing and Accountability governs data auditing guidelines and requirements and defines the events as well as the content that must be included. Date/Time, component, type, user, and outcome make up the required audit record. It should be noted that all cloud partners may not be able to adhere to CJIS guidelines to obtain certification due to size and cost so this is not a requirement, however is the standard which to strive for.

2. Surveillance data should be deleted within one year or less. Narrow exceptions can be made for specific data required for prosecution, legal cases or other narrow government purposes. Such exceptions must be approved by the Chief of Police or the City Manager.

Proposed change: Surveillance video data shall follow a one-year retention policy

City Council Comment Summary: Can data be stored for less than one year, such as fourteen days?

CAO Response: If the data collected by the surveillance technology is video only, then under Government Code § 34090.6, the City may only delete videos after it has retained the video footage for one year. However, if the information is an audio recording, it need only be retained for 100 days. The City may be required to retain the video data collected even longer

than a year, if the video recording is identified as evidence of a crime or related to a citizen complaint or internal investigation, per the Police Department's Records Retention Schedule.

3. Surveillance data should not be stored in The Cloud.

Proposed change: Surveillance data may be stored in the cloud if the vendor can demonstrate strict standards, encryption, redundancy, and access such as those outlined by the FBI CJIS Security Policy.

City Council Comment Summary: The public sector uses cloud storage technology which includes public safety. If data is stored in the cloud, then strict standards need to be followed for encryption, redundancy, and access.

UAS Application Response:

Data stored from this program is housed in a CJIS certified cloud environment. The FBI Criminal Justice Information Services (CJIS) Security Policy provides a set of security requirements to protect and safeguard Criminal Justice Information (CJI) used by law enforcement. There are 13 Policy areas which cover a range of requirements including security training, personnel and physical security, data protection and integrity. For example, Amazon and Microsoft both offer CJIS compliant cloud hosted solutions and publicly advertise their compliance.

Examples of Core Cloud Requirements
a. Adhere to CJIS security policy 5.8 standards: Media Protection which covers media storage, access, transport, sanitation, and disposal.
b. Encryption of data at rest and in transit (CJIS Requirement)
c. Data Redundancy (CJIS Requirement)
d. Limited and Controlled Access (CJIS Requirement)

4. If 3rd party companies are used to collect or store surveillance data, then those companies must be contractually required to protect that data in accordance with our policies.

City Council Comment Summary: Can language be added that states we need to know who accesses data in writing, no sale of data, transfer of data, or anything else is permitted? Can we also add language which gives the City the right to audit these 3rd party companies?

CAO Response: Whenever the City contracts with an outside company for services, the City can negotiate the terms of a contract, to a degree. For instance, in previous contracts with Axon, who provides the body warn camera devices for HPD, a "privacy" clause in the contract indicates that Axon cannot disclose agency content or information "except as compelled by a court or administrative body or required by law or regulation," and that Axon must provide notice to the agency if disclosure is provided, so that an objection can be filed. This clause also limits Axon's "access to certain information from Agency" to simply performing troubleshooting services upon request, enforce the agreement or conduct an evaluation of the system.

Additionally, standard contracts with the City of Hayward always include an "Assignment" Clause, indicating that the company providing services cannot assign others to do its job, and the contracts can include non-disclosure agreements, prohibiting the service company from disclosing, transferring or selling information it receives while operating for the City, without City approval.

Finally, the City has, on numerous occasions, negotiated with service companies regarding the retention of ownership rights and the ability to audit. Standard language for retaining ownership of data could indicate the following:

> *Subject to the rights granted in this agreement, the City of Hayward and its licensors retain all right, title and interest in and to the data and information obtained via the use of a drones and Contractor acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement.*

Standard language for a right-to-audit clause could indicate the following:

> *The City of Hayward may conduct an audit of Contractor's financial, performance and compliance records maintained in connection with the operations and services performed under this Contract. In the event of such audit, Contractor agrees to provide the City with reasonable access to Contractor's employees and make all such financial, performance and compliance records available to the City.*

C. Use and Dissemination

1. Use of surveillance data should be restricted to legitimate law enforcement uses.

City Council Comment Summary: City Attorney's office review of this language is requested. Since the City owns the data, must the City grant consent?

CAO Response: Under the law (including the law explained in Section A, subsection 3), the City of Hayward is obligated to only use UAVs for legitimate law enforcement purposes. As explained above, in most circumstances, HPD will be required to obtain a warrant for use of a UAV, unless an emergency or exigency type situation occurs, or no Fourth Amendment rights are implicated (the object being surveilled is in plain sight/public view). Moreover, the City has no intent to allow any data obtained via use of surveillance technology to be used for any purpose other than legitimate law enforcement purposes, unless the City is ordered to produce such per a Court order or an order from another type of judicial body. In that regard, the City is able to contract to retain ownership of all data gathered when surveillance technology is used, in order to make sure access to that data is limited.

2. Access to surveillance footage of any kind should be protected and restricted to Hayward law enforcement personnel.

City Council Comment Summary: City Attorney's office review of this language is requested. The person or team should be identified.

CAO Response: As indicated above, it is standard, in contracts with companies whose services may disclose personal information, that the City include a "privacy" clause in its contract, limiting the ability of the public to view certain items. As noted above, in our contract with Axon for Body Worn Cameras, we included language which prohibits Axon from disclosing information to anyone, unless there is an order by a court or administrative body, or disclosure of the information is otherwise required by law (for instance if a Public Records Act request is made). As such, generally, access to the surveillance footage will be limited to Hayward law enforcement, unless the City is ordered otherwise or the City has a legal duty to release the data.

3. The sharing of surveillance data with other agencies (local, state and federal) should be severely restricted to protect the privacy rights of our residents.

CAO Response: It is the City's practice to protect the privacy rights of our citizens, while also recognizing that the sharing of information between law enforcement agencies can be very beneficial to public safety. In that regard, the City already attempts to restrict access to private information of its citizens, to the best of its ability, given the state of the law by meeting and conferring with information requestors to find alternative solutions, or objecting to the requests. However, the creation of the Public Records Act, SB 1421 and AB 748, which require the disclosure of surveillance type data (body worn camera footage, statistical data, etc.) the City is unable to restrict such sharing of information "severely," unless there are grounds for objecting to the request or the material requested is exempt from disclosure.

4. If 3rd party companies are used to collect or store surveillance data, then they may not share that data with anyone without the City of Hayward's express, written consent.

City Council Comment Summary: City Attorney's office review of this language is requested. Stricter language is requested.

CAO Response: The City has the ability to negotiate a separate Non-Disclosure Agreement, or to include a Non-Disclosure Agreement clause in the contract, which would prohibit the sharing or sale of data by third parties without the City's consent.

5. Surveillance data collected by law enforcement should not be subject to PRA requests, unless the request is narrow and specific to a particular incident.

City Council Comment Summary: City Attorney's office review of this language is requested.

CAO Response: Unfortunately, the City is not able to create its own local law which contradicts/conflicts with state laws/statutes, which includes the Public Records Act (PRA) (California Government Code § 6250). The PRA provides the public with the ability to request information from the City, some of which the City must disclose. As indicated in the PRA, in creating the act the legislature found "and declare(d) that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state," meaning the legislatures desire in creating the PRA was transparency between local government and its citizens. San Gabriel Tribune v. Superior Court (1983) 143 Cal. App. 3d 762, 771 That said, the City is not obligated to produce material if the request made is not narrow or specific. However, under the PRA, the City has an obligation to meet and confer with/assist the requester to help the request narrow or specify their request. Government Code § 6253.1. In that regard, the City does not ever produce material requested under the PRA if the request is not narrow and specific.