CITY OF OAKLAND

Privacy Advisory Commission

May 2, 2019 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Vacant, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Vacant, **Mayoral Representative**: Heather Patterson*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. 5:00pm: Call to Order, determination of quorum

2. 5:05pm: Open Forum/Public Comment

3. 5:10pm: Review and approval of the draft April 4 meeting minutes

4. 5:15pm: UC Berkeley's Samuelson Law, Technology & Public Policy Clinic – presentation of draft Privacy Principles; review and take possible action.

5. 5:30pm: Federal Task Force Transparency Ordinance – OPD – presentation of inaugural annual report for FBI/JTTF; review and take possible action.

6. 5:40pm: Surveillance Equipment Ordinance – Hofer/Patterson – proposed amendment to prohibit use of facial recognition technology; review and take possible action.

7. 6:00pm: Surveillance Equipment Ordinance – OPD – Remote Camera Impact Report and draft use Policy – review and take possible action.

8. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

April 4, 2019 5:10 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Vacant, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Vacant, **Mayoral Representative**: Heather Patterson*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. 5:10pm: Call to Order, determination of quorum

Members Present: Hofer, Jacquez, Katz, Suleiman, Oliver.

2. 5:15pm: Open Forum/Public Comment

Although there were no public speakers, Chairperson Hofer took this opportunity to honor the participation of former Member Saied Karamooz who stepped off the commission last month.

3. 5:20pm: Review and take possible action on the OPD Automated License Plate Reader Anticipated Impact Report and draft Use Policy.

Chairperson Hofer entertained public speakers first on this item. J.P. Masser provided a written letter and also spoke about inconsistencies in the policy that he is concerned with. He asked if the intent was to use ALPEs for all crime, serious felonies, or even just in routine patrol operations. He noted that LPR use amounts to mass surveillance of people without any probable cause to surveil most of them.

Member Katz echoed some of his concerns and noted that the system scoops up data at an alarming rate. Member Jacquez also noted his concern about the retention of data which the department currently discards after 6 months.

Lt. Robert Rosen presented on behalf of OPD and noted that as a 14-year veteran with 8 years as an investigator and 6 years working on solving homicides, he uses ALPR Data every day. He noted that the process for using the tool is very transparent and that no random surveillance of the data is allowed by the department. Each investigation starts with a specific piece of information that the officer is looking for and they must log in every use of the system and explain why they are using it. In order to query the system, it requires an incident number to be entered.

The Commission still had questions about data retention schedules, auditing capabilities, and allowable uses. They articulated a desire to have a specific list of allowable uses similar to the DAC Policy that was adopted prior to the PAC Creation. The item was continued to the May meeting to allow staff to provide further clarification in the proposed use policy.

4. 6:00pm: Review and take possible action on the OPD Remote Camera Impact Report and draft Use Policy.

Bruce Stoffmacher presented the Impact Assessment and proposed Use Policy for discussion. He noted that currently OPD has 4 transmitters and a number of consumer grade cameras and the department hopes to replace 4 older cameras and add 6 new pole cameras with an upcoming JAG Grant. The Policy and Impact Statement contemplate two very different situations for use: 1) The Pole Cameras can be affixed to Utility Poles for specific covert operations (often with a prior court order) and monitored remotely. 2) the cameras can be "hand held" by officers in large scale events during which situational awareness is critical to protect public safety. Because these types of cameras can be controlled/monitored from afar, they fall under the surveillance technology ordinance for review and approval.

The Commission asked several clarifying questions about the type of cameras, the transmitters, and the contract with an outside vendor. The direction given to staff was to separate out the uses in the policy and bring refined documents back in May.

5. 7:00pm: Adjournment

City of Oakland Privacy Principles

Oakland is a diverse city with a history of active civic participation on issues of privacy and surveillance. As we evolve, it is imperative that we learn from both the positive and negative aspects of our past to build our future. Progress at the expense of personal privacy and safety is unacceptable. We recognize the need to protect Oaklanders' privacy as city services incorporate emerging technologies.

Privacy is a fundamental human right, a California state right, and instrumental to Oaklanders' safety, health, security, and access to city services. We seek to safeguard the privacy of every Oakland resident in order to promote fairness and protect civil liberties across all of Oakland's diverse communities. In all situations, we pledge to handle personal information in a manner that builds trust and preserves Oaklanders' privacy and safety. The following Privacy Principles guide our actions.

DESIGN AND USE EQUITABLE PRIVACY PRACTICES

Community safety and access to city services should not come at the expense of any Oaklander's right to privacy. We recognize that our collection and use of personal information has disadvantaged marginalized communities at different periods during Oakland's history. We aim to avert future inequities by collecting information in ways that do not discriminate against any Oaklander or Oakland community. When possible, we will offer clearly communicated alternatives to the collection of personal information at the time of collection.

LIMIT COLLECTION AND RETENTION OF PERSONAL INFORMATION

We believe that we should collect and store personal information only when and for as long as is justified to directly serve the specific purpose for which it is collected, such as to protect Oaklanders' safety, health, or access to city services. We will continue our practice of reaching out to Oaklanders for their views on the information we collect and how we use it. We also will look for new opportunities for outreach.

MANAGE PERSONAL INFORMATION WITH DILIGENCE

The personal information of Oaklanders should be treated with respect. We handle all personal information in our custody with care, regardless of how or by whom it was collected. To maintain the security of our systems, we review and regularly update software and applications that interact with Oaklanders' personal information. Further, we recognize that deletion, encryption, minimization, and anonymization can reduce misuse of personal information. We aim to make effective use of these tools and practices. Additionally, we combine personal information gathered from different departments only when we must.

EXTEND PRIVACY PROTECTIONS TO OUR RELATIONSHIPS WITH THIRD PARTIES

Our responsibility to protect Oaklanders' privacy extends to our work with vendors and partners. Accordingly, we share personal information with third parties only when necessary to provide city services, and only when doing so is consistent with these Principles. When the law permits, we will disclose the identity of parties with whom we share personal information.

SAFEGUARD INDIVIDUAL PRIVACY IN PUBLIC RECORDS DISCLOSURES

Open government and respect for privacy go hand-in-hand. Providing relevant information to interested parties about our services and governance is essential to democratic participation and civic engagement. We will protect Oaklanders' individual privacy interests and the City's information security interests while still preserving the fundamental objective of the California Public Records Act to encourage transparency.

BE TRANSPARENT AND OPEN

Oaklanders' right to privacy is furthered by the ability to access and understand explanations of why and how we collect, use, manage, and share personal information. To that end, we aim to communicate these explanations to Oakland communities in plain, accessible language on the City of Oakland website. We also aim to communicate this information at a time when it is relevant and useful.

BE ACCOUNTABLE TO OAKLANDERS

Trust in our stewardship of personal information requires both that we collect and manage personal information appropriately, and that we create opportunities for active public participation. We publicly review and discuss departmental requests to acquire and use technology that can be used for surveillance purposes. We encourage Oaklanders to share their concerns and views about any system or department that collects and uses their personal information, or has the potential to do so. We also encourage Oaklanders to share their views on our compliance with these Principles.

Implementation Guidance: City of Oakland Privacy Principles

This document accompanies the City of Oakland's Privacy Principles (the "**Principles**"). It provides guidance on the implementation of the Principles, including a discussion of the foundation and scope of each principle, as well as examples to illustrate how the City might apply each Principle in its day-to-day operations.

The goals of the Principles are threefold. First, the Principles serve as a values statement establishing how the City protects Oaklanders' privacy and security. Second, the Principles will help guide the development of future privacy policies for the City. Third, the Principles are intended to harmonize the way different City departments think about privacy when approaching a new technology or a new issue with data collection.

The Principles open with a preamble that establishes the purpose and tone of the Principles. The Principles themselves are organized into seven different categories: (1) Equity; (2) Collection and Retention; (3) Management of Personal Information; (4) Third Party Relationships; (5) Public Records Disclosures; (6) Transparency; and (7) Accountability. This guidance document contains separate sections for each Principle, explaining its purpose and foundation, as well as providing examples of how each Principle applies to specific situations. The examples are intended to illustrate how City departments would take the Principles into account, rather than to dictate the result that consideration of the Principles would require.

DESIGN AND USE EQUITABLE PRIVACY PRACTICES

Community safety and access to city services should not come at the expense of any Oaklander's right to privacy. We recognize that our collection and use of personal information has disadvantaged marginalized communities at different periods during Oakland's history. We aim to avert future inequities by collecting information in ways that do not discriminate against any Oaklander or Oakland community. When possible, we will offer clearly communicated alternatives to the collection of personal information at the time of collection.

I. Purpose and Goals of the Equity Principle

The Equity Principle guides the City of Oakland's commitment to collect and use personal information equitably across communities and groups in the course of providing city services. The Principle acknowledges that at different points in Oakland's history, marginalized communities have faced disproportionate surveillance or other intrusions into their privacy.[1] It also recognizes the importance of respecting Oaklanders' choices in whether and how their personal information is collected and used by the City. As the Principle explains, "[the City will] aim to avert future inequities by collecting information in ways that do not discriminate against any Oaklander or Oakland community." Therefore, the City will not collect information in unfair ways that target specific communities or neighborhoods, or overlook—and thereby risk perpetuating—past discrimination.[2] The City already takes steps to prevent the unfair targeting of certain groups by following the state's sanctuary law, the California Values Act, which prevents local law enforcement from aiding federal agencies in deportations.[3]

Equal protection under the law is ensured at the federal, state, and local levels. The Fourteenth Amendment of the United States Constitution guarantees the equal protection of all persons under the law.[4] The California Constitution contains its own equivalent equal protection clause, which states that a "person may not be deprived of life, liberty, or property without due process of law or denied equal protection of the laws."[5]

---

[1] *See* Catherine Crump, *Surveillance Policy Making by Procurement*, 91 Wash. L. Rev. 1595, 1617–18 (2016) (describing how the Black Panther Party became a target of the FBI's COINTELPRO surveillance investigation in the 1960s).

[2] The City of Oakland defines fairness to mean "that identity—such as race, ethnicity, gender, age, disability, sexual orientation or expression—has no detrimental effect on the distribution of resources, opportunities and outcomes for our City's residents." City of Oakland, *Oakland Equity Indicators: Measuring Change Toward Greater Equity in Oakland* at 8 (2018) [hereinafter "*Equity Indicators Report*"], https://s3-us-west-1.amazonaws.com/beta.oaklandca.gov/pdfs/2018-Equity-Indicators-Full-Report.pdf.

[3] Cal. Gov. Code § 7284–7284.12 (effective Jan. 1, 2018).

[4] U.S. Const. amend. XIV, § 1.

[5] Cal. Const. art. I, § 7.

The City of Oakland's own commitment to equity is illustrated by its pioneering partnership with the City University of New York's Institute for State and Local Governance to develop an Equity Indicators tool.[6] The Department of Race and Equity developed the Oakland Equity Indicators Report in order to help City staff "make data-driven decisions about programs and policies to . . . ensure people have equitable access to opportunities and services that we administer or deliver, directly or by contract."[7] The City of Oakland distinguishes equality—"giving everyone the same thing, regardless of outcomes"—from equity, which means "ensuring that people have access to the same opportunities or services[.]"[8] The City also fosters equity through its "Equal Access to Services" ordinance, which establishes standards and procedures to help Oaklanders with limited proficiency in English can access city services and programs.[9]

The Equity Principle brings the same values that animate these efforts to the City's protection of residents' privacy interests.

II. Examples Illustrating the Equity Principle in Practice

Example #1: Education and Chronic Absenteeism

The Oakland Unified School District ("**OUSD**") wants to measure the percentage of students who are chronically absent. Studies have shown that chronic absenteeism significantly affects a child's ability to succeed in school and therefore influences a child's access to later opportunities and success.

Since the purpose of the measurement is not to enforce truancy laws against any student or their parents, OUSD does not collect names or other personal information. Therefore, OUSD decides to collect only the demographic data associated with students whose attendance rate is 90% or less (missing 18 or more days in a 180-day school year), regardless of whether the absences are excused or unexcused. Following the Equity Principle's guidance, OUSD also gives parents the choice to opt-out of collection of racial or other demographic information.

Example #2: Department of Transportation and Mobile Automated License Plate Readers

The Department of Transportation ("**DOT**") wishes to employ vehicle-mounted Automated License Plate Readers ("**ALPR**") in order to manage and enforce parking violations. Before getting approval from the City Council to fund the acquisition, DOT presents an Anticipated Impact Report and Use Policy for the Privacy Advisory Commission ("**PAC**") to review and make a recommendation to the City Council.

---

[6]. *Equity Indicators Report* at 8.
[7]. *Id.* at 12
[8] City of Oakland, *Learn More about the Department of Race and Equity*, *available at* https://www.oaklandca.gov/resources/race-matters (last visited Apr. 26, 2019).
[9] Oakland, Cal., Ordinance 12324 § 2.30.030.

DOT is aware of the community concern about having ALPR on at all times while the vehicle is moving through marginalized communities. With that concern in mind, DOT decides that it will turn on ALPR only when patrolling the areas in which parking violations occur, which are largely commercial districts and neighborhoods with Resident Permit Parking areas. To further address the concern, DOT provides anonymized data to the Department of Race and Equity to audit and help determine whether the collection is having a disparate impact.

Example #3: Libraries and Surveillance Cameras

The Oakland Public Library receives extra funding and a mandate to install surveillance cameras at several of its branches. The Library considers installing the new cameras in the branches with the highest number of incidents. However, it recognizes that this metric will predominantly affect marginalized communities.

The Library wants to proactively address how cameras affect the branches' visitors, so it reaches out to PAC with its concerns. At the same time, library branches institute a comment box policy so patrons can submit their thoughts on the use of surveillance cameras in each branch anonymously. Only after considering both the insight from PAC and the collective patron feedback does the Oakland Public Library determine whether and where to place the new cameras.

LIMIT COLLECTION AND RETENTION OF PERSONAL INFORMATION

We believe that we should collect and store personal information only when and for as long as is justified to directly serve the specific purpose for which it is collected, such as to protect Oaklanders' safety, health, or access to city services. We will continue our practice of reaching out to Oaklanders for their views on the information we collect and how we use it. We also will look for new opportunities for outreach.

I. Purpose and Goals of the Collection and Retention Principle

Considering the privacy implications of collecting personal information before the collection begins helps prevent privacy violations. And thoughtful retention is just as relevant to protecting individual privacy as collection. The Collection and Retention Principle affirms the City of Oakland's commitment to limit its collection of personal information, collecting only what is needed in order to provide a city service and only for as long as required. By stating that personal information will be collected "only when and for as long as is justified," the Principle helps ensure that personal information will not be used in unintended or unexpected ways. This approach prevents the City from misusing "sleeping data," which includes stored or unused data that is digitized and then repurposed for an unforeseen use. The Principle also reflects the importance of outreach to the democratic process: residents should be able to voice concerns both before and after information is collected.

This Principle guides data collection and retention within the boundaries of existing law. The State Records Management Act directs the California Secretary of State to establish and administer a records management program, which includes the retention and disposal of state records.[10] Section 12275 of the Act provides that "[a] record shall not be destroyed or otherwise disposed of by an agency of the state, unless . . . the record has no further administrative, legal, or fiscal value and . . . the record is inappropriate for preservation in the State Archives."[11] Under the Act, government agencies must establish and maintain a records retention schedule.[12] The schedule must detail what records the agency will keep, how the records will be managed, and how the agency will legally dispose of non-permanent records.[13] At the local level, cities must retain any record that is less than two years old.[14] However, records of "routine video monitoring" may be destroyed after one year and recordings of telephone and radio communications may be destroyed after 100 days with approval from city council and the written consent of the

[10] Cal. Gov. Code §§ 12270–79.
[11] Cal. Gov. Code § 12275.
[12] Cal. Gov. Code § 12274.
[13] *Id.*
[14] Cal. Gov. Code § 34090.

city attorney.[15] Duplicates less than two years old may be destroyed if they are no longer required.[16]

II. Examples Illustrating the Collection and Retention Principle in Practice

Example #1: Fire Department and Body Heat Cameras

The Oakland Fire Department wants to add body-worn cameras to firefighter uniforms in order to aid in search and rescue. Because the Fire Department wants to use the body-worn cameras to help search and rescue operations, it determines that the cameras do not need to record live footage, which would record images of the immediate surroundings and any persons within the camera view. Instead, the Fire Department decides that cameras that record only heat signatures are sufficient to help firefighters find and rescue Oaklanders who may be trapped in a fire.

The Fire Department introduces the heat signature cameras in its search and rescue operations. All recordings are retained according to the department's retention schedule and then destroyed.

Example #2: Libraries Collecting Less Patron Data

The Oakland Public Library collects the name, date of birth, address, gender, phone number, and other personal information from patrons when applying for a library card. Whenever a patron checks out a book, that book is tied to the patron information associated with that patron's account.

The Library decides to redouble its efforts to foster community and move away from generating revenue from lending activities. As a result, fine collection for overdue books becomes less of a priority. Additionally, in view of the USA PATRIOT Act's provision granting law enforcement access to patron records in certain circumstances,[17] the Library decides to limit its collection of information so as not to be subject to requests from agencies, knowing that the information could be used to target vulnerable patrons. The Library decides to collect only first and last names, for which a patron may use an alias, and dates of birth. A patron is not required to provide an address or phone number but may choose to do so. Thus, when a patron checks out a physical book, it is tied only to the information associated with the patron's library card.

Example #3: Public Health and Childhood Asthma

The Department of Race and Equity wants to measure the rates of asthma-related emergency visits to hospitals in the Oakland area in order to determine racial disparities in the incidence of

[15] Cal. Gov. Code § 34090.6.
[16] Cal. Gov. Code § 34090.7.
[17] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, § 215 (2001).

asthma in children for the Equity Indicators Report. Childhood asthma has been linked to poor housing conditions, and the Department wishes to explore that connection in its report.

Cognizant of the privacy and safety concerns associated with a child's personal information, the Department of Race and Equity decides to collect only the race and residential data for asthma-related emergency room visits for children under five years of age. Rather than collecting each child's name and address, the Department decides to collect only zip codes and census block data, which is sufficient to determine the housing conditions of neighborhoods. The Department also puts in place a retention schedule for eventual deletion of the information.

MANAGE PERSONAL INFORMATION WITH DILIGENCE

The personal information of Oaklanders should be treated with respect. We handle all personal information in our custody with care, regardless of how or by whom it was collected. To maintain the security of our systems, we review and regularly update software and applications that interact with Oaklanders' personal information. Further, we recognize that deletion, encryption, minimization, and anonymization can reduce misuse of personal information. We aim to make effective use of these tools and practices. Additionally, we combine personal information gathered from different departments only when we must.

I. Purpose and Goals of the Management of Personal Information Principle

The Management Principle affirms the City of Oakland's commitment to protect the privacy of residents' personal information once that information has been collected by the City. Responsible data management helps the City build trust: The City can provide better services to Oaklanders if Oaklanders feel more secure in the handling of information shared with the City. To that effect, the Management Principle covers the storage, security, and accessibility of personal information of Oakland residents with a specific focus on information security practices. How the information is collected is irrelevant to these practices, which come into play once information becomes part of the City's records. Additionally, the Management Principle limits aggregation of personal information across different City departments to those instances where aggregation is necessary for the City to provide services.

Minimization, encryption, anonymization, and deletion are identified in the Management Principle because these are best practices for information management. Data minimization is the act of following a purpose-specific approach to collecting data and gathering only the data necessary to provide city services. Encryption is the process of encoding data to prevents access by unauthorized individuals. Anonymization is the process by which personal data is obscured to inhibit deriving from data the identity of the individual who provided it. Deletion is the act of deleting any information that is not necessary for the City to provide services to residents.

The newly enacted California Consumer Privacy Act ("**CCPA**") gives California consumers the right to demand that business delete personal information collected from that consumer.[18] It also provides a list of measures to protect personal information, including pseudonymization and deidentification.[19] Collectively, these provisions show the importance of technological safeguards to protect individual privacy. The Management Principle similarly identifies available measures to protect Oakland residents' personal information that the City collects and stores.

---

[18] *See* California Consumer Privacy Act of 2018, L. 2018 ch. 55 (A.B. No. 375), codified at Cal. Civ. Code § 1798.100 *et seq.*, § 1798.105(a) [hereinafter **"CCPA"**]. The CCPA is currently undergoing amendment and becomes operative January 1, 2020.

[19] *See* CCPA §§ 1798.100, 1798.140, 1798.145.

The Principle's direction to "make effective use" of these measures implies that use of those measures, and others, will evolve over time.

II. Examples Illustrating the Management Principle in Practice

Example #1: City Clerk's EMT Records

An employee at the City Clerk's Office received an automated notice from Alameda County regarding an Oakland resident's use of Emergency Medical Technician (**"EMT"**) services. The Oakland resident had suffered a heart attack and another Oakland park visitor had called emergency services, which routed to the County EMT hotline. The County hotline dispatched an ambulance to the scene. Because of the healthcare implications, the paramedics on duty collected a substantial amount of health information about the patient, including the patient's name, date of birth, medical history, current medications, insurance information, and emergency contacts.

Because all the information collected is personal information, privacy concerns about the safety and security interests of Oakland residents are implicated. In order to best protect the privacy of the individual who suffered the heart attack and of the individual who placed the call to emergency services, the employee at the City Clerk's Office followed Oakland City policy and shredded all the personal information included in the notice.

Example #2: Primary Languages and ICE

To improve classroom outcomes, administrators at several schools in the Oakland Unified School District (**"OUSD"**) want to conduct a survey about primary languages spoken in the home of students enrolled in Head Start programs. The administrators create a survey working group made up of teachers from different schools within the Oakland community. Despite the fact that Oakland has passed a Sanctuary City Ordinance that prevents the City's departments and officials from turning over immigration information to Immigration and Customs Enforcement ("**ICE"**), the group is concerned that this survey data can be used by other federal law enforcement agencies to collaborate with ICE and target neighborhoods for immigration enforcement.

To respond to this concern, the working group proactively anonymizes the results and removes personal information that can be used to reverse-engineer identities from the information collected. Additionally, since this will be a multi-school survey, the group codes the results such that individuals not involved in the administration of the survey will not be able to determine data for specific schools without OUSD's involvement and approval. Finally, school administrators verify that the server storing the survey data has been updated with the latest security patches.

Example #3: Public Works Volunteer Program Application Process

An employee at the Department of Public Works has been tasked with creating a volunteer program that provides opportunities to help beautify Oakland neighborhoods and clear city drains. The Department of Public Works wants to make this Adopt-a-Drain Program accessible to all Oaklanders in order to create a database of potential volunteers for future projects. To create the

volunteer database, the Department of Public Works has to collect substantial amounts of personal information about the applicants, some of which is highly sensitive.

Recognizing the importance of ensuring the privacy and security of individuals applying to be volunteers, the Department of Public Works collaborates with the IT Department from an early stage to design a secure application system for the Adopt-a-Drain Program. The application system is regularly updated and protected from being accessed by unauthorized parties. The Department also informs all potential applicants about this new, protective application portal on the application website.

EXTEND PRIVACY PROTECTIONS TO OUR RELATIONSHIPS WITH THIRD PARTIES

Our responsibility to protect Oaklanders' privacy extends to our work with vendors and partners. Accordingly, we share personal information with third parties only when necessary to provide city services, and only when doing so is consistent with these Principles. When the law permits, we will disclose the identity of parties with whom we share personal information.

I. Purpose and Goals of the Third-Party Relationships Principle

In the course of providing city services, the City sometimes must exchange personal information with third parties. The Third-Party Relationships Principle extends the City's commitment to protect Oaklanders' privacy to parties that work with the City. The City engages with a range of vendors and partners that fall into two broad categories: City entities and non-City entities. The City will share personal information with these third parties—whether City or non-City entities—only to the extent necessary to provide city services, and to the extent that this sharing adheres to all of the other Principles and applicable laws.

The first category of third-party relationships describes relationships between entities within the City. In general, this category refers to instances in which two or more City departments enter into partnerships involving the exchange of personal information in order to provide city services to residents. These intra-city relationships typically are not governed by a contract and do not involve the exchange of money for goods or services.

The second category of third-party relationships describes relationships between the City and non-City entities. This category is much broader and encompasses the City's relationships with both public and private parties. The City may partner with other public entities outside of Oakland, including departments and agencies in other cities, or at the state, county, or federal levels. The City also enters into contractual, paid relationships with private non-City entities. For example, the City regularly issues requests for proposals from private vendors, who have the opportunity to bid on public projects ranging from the provision of new law enforcement technology to sidewalk repairs and park maintenance.

The City must abide by a variety of contracting policies and legislation when entering into an agreement that might involve information sharing with a third party.[20] Further, Oakland's Sur-

[20] City of Oakland, Contracting Policies and Legislation, https://www.oaklandca.gov/resources/contracting-policies-and-legislation/ (last visited Apr. 1, 2019). For example, in 2001, the City passed an ordinance preventing city contractors under contracts of at least $25,000 from discriminating in the provision of benefits between employees with spouses and employees with domestic partners. *See* Oakland, Cal., Mun. Code § 2.32.010–2.32.110.

veillance Technology Ordinance ("**Surveillance Ordinance**") contains provisions applicable to certain types of third-party information sharing.[21] In general, City Council approval is required whenever the City wishes to enter into a contract with a non-City entity to use surveillance technology, which includes approval for data sharing agreements.[22] The Surveillance Ordinance also requires the City to produce an impact report for each technology it wishes to acquire, including a discussion of potential third party dependencies in handling and storing information generated by the technology.[23] Similarly, the Surveillance Ordinance requires the city to draft a surveillance use policy for each technology it wishes to acquire, which must include a discussion of a policy for third-party data sharing with both City and non-City entities.[24] Lastly, once the City begins to use a particular surveillance technology, the Surveillance Ordinance requires an annual surveillance report, including a discussion of what data was collected and shared with outside entities during use of the technology.[25]

II. Examples Illustrating the Third-Party Relationships Principle in Practice

Example #1: Information Sharing with FEMA After a Wildfire

A major wildfire recently broke out in the Oakland Hills and caused widespread damage. The Oakland Fire Department coordinated with other local and state departments on fire relief efforts, but the extent of damage necessitates federal assistance once the fire is extinguished. The City of Oakland begins conversations with the Federal Emergency Management Agency ("**FEMA**") about receiving federal funding for its disaster recovery efforts. In order to qualify for a grant, the City must provide FEMA with certain information about the number of homes and families impacted, including addresses of these homes and the names of known occupants.

In compiling this file for FEMA, the City gathers only the minimum information necessary to receive the funding. In so doing, it redacts any personal information—such as household income and citizenship status—not relevant to the impact assessment FEMA will need to conduct.

Example #2: Data Sharing Agreement with ALPR Vendor

The City of Oakland, through the Oakland Police Department ("**OPD**"), begins contract negotiations with LicenseCam, a vendor of Automatic License Plate Recognition ("**ALPR**") technology. As part of the contract, LicenseCam requests that the City provide monthly success metrics quantifying how frequently the ALPR technology has helped OPD locate a person of interest. LicenseCam also requests that the City provide the raw data—including images of license plates, makes and models of cars, and names of car registrants—to corroborate these statistics.

---

[21] *See* Oakland, Cal., Mun. Code § 9.64.010–9.64.070.
[22] Oakland, Cal., Mun. Code § 9.64.030(1)(D).
[23] Oakland, Cal., Mun. Code § 9.64.010(6)(I).
[24] Oakland, Cal., Mun. Code § 9.64.010(7)(H).
[25] Oakland, Cal., Mun. Code § 9.64.010(1)(B).

This data sharing agreement is put up for review before the Oakland Privacy Advisory Commission ("**PAC**") in advance of a vote by the City Council. Based upon feedback from PAC, the City modifies the data sharing agreement to state that OPD agrees to disclose the monthly hit rates of LicenseCam, but does not agree to share the information underlying these statistics. OPD reaches this policy decision by concluding that sharing personal information with LicenseCam is not necessary to provide law enforcement services to Oakland residents.

Example #3: Data Sharing Between City Departments

There has been a massive uptick in car break-ins throughout the City of Oakland, particularly in large parking lots adjacent to BART stations, libraries, and event spaces. In an effort to address the situation, OPD requests CCTV video footage from a list of City Departments and divisions known to operate CCTV cameras, including the Department of Transportation, the Oakland Public Library, and the Oakland-Alameda County Coliseum Authority.

Since OPD wishes to gather only the information necessary to resolve the current uptick in car break-ins, it makes clear in its requests to other City entities its commitment to use this video footage only in connection with that specific objective. It also makes a commitment to purge the aggregated video footage per OPD's approved retention schedule.

SAFEGUARD INDIVIDUAL PRIVACY IN PUBLIC RECORD DISCLOSURES

Open government and respect for privacy go hand-in-hand. Providing relevant information to interested parties about our services and governance is essential to democratic participation and civic engagement. We will protect Oaklanders' individual privacy interests and the City's information security interests while still preserving the fundamental objective of the California Public Records Act to require transparency.

I. Purpose and Goals of the Public Records Principle

The Public Records Principle affirms the City of Oakland's commitment to take specific steps to safeguard its residents' privacy when complying with public records requests, and to consider whether and how it will comply with requests where the disclosure could include personal information. While the California Public Records Act ("**CPRA**")[26] already includes privacy and security protections, many of these exemptions are invoked at the discretion of the agency or government entity receiving the request. This Principle helps guide the exercise of that discretion. As the Principle explains, "[o]pen government and respect for privacy go hand-in-hand." The City recognizes its residents' strong and sometimes competing interests in transparency and personal privacy and security, and it is committed to weighing these interests carefully when complying with CPRA requests.

In considering whether the public interest weighs in favor of disclosure, the City will keep top of mind its commitment to foster "democratic participation and civic engagement" through transparency. These words convey the strong interest in disclosing information relevant to matters of public debate or interest. On the other hand, in situations where the City determines the public interest in privacy and security requires redaction of an individual's personal information prior to disclosure of a record, the City will redact in a manner that fully protects the information identified as sensitive. The City will use care in making decisions about redactions where the information requested may not amount to "personal information" in isolation, but may rise to the level of "personal information" if aggregated with other public records.

California enacted the CPRA to implement Californians' fundamental right to access information concerning the conduct of the People's business.[27] While the state passed the law with increased transparency in mind, it also took note of the privacy and security implications that come with increased transparency. In fact, the statute references privacy in its opening sentence: "In enacting this chapter, the Legislature, *mindful of the right of individuals to privacy*, finds and declares that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state."[28]

---

[26] Cal. Gov't. Code §§ 6250–76.48

[27] Cal. Gov't. Code § 6250.

[28] Cal. Gov't. Code § 6250 (emphasis added).

Multiple provisions of the CPRA include privacy-related exemptions that give agencies discretion to either not disclose certain information or limit the information disclosed. When exercising its discretion to exempt information from disclosure on the ground that disclosure would constitute an unwarranted invasion of privacy, the agency must weigh the public interest in disclosure against the public interest in privacy and security.[29] The Public Records Principle is intended to guide that exercise of discretion in a way that best furthers twin objectives of transparency and privacy.

II. Examples Illustrating the Public Records Principle in Practice

Example #1: Redacting Documents Responsive to Broad Public Records Requests

A resident submits a CPRA request seeking all emails sent and received by the City in 2018 discussing use of Oakland Paratransit Services. The City receives this request, completes the requisite search, and compiles a file of all relevant emails. However, the file the City compiles contains a set of emails between employees in the Department of Human Services discussing specific residents and their travel routines. The emails contain the full names of many users of paratransit services.

While the City understands the importance of disclosing the records requested, it also considers the privacy implications of disclosing this small subset of emails containing sensitive personnel information about potentially vulnerable residents. In weighing disclosure against privacy, the City determines it must withhold the names and location information of paratransit users.

Example #2: Maintaining Privacy During Law Enforcement Investigations

A reporter submits a CPRA request to the Oakland Police Department seeking any video footage it has of a recent incident in West Oakland that resulted in a police officer discharging his firearm after being called to the scene to investigate an alleged altercation. The City locates the relevant Police Department body camera footage, but upon reviewing it, realizes the altercation in question took place next door to the West Oakland Planned Parenthood. Because of the angle of the camera, it caught footage not only of the altercation, but also of people walking in and out of the Planned Parenthood behind the scene of the dispute.

Since the altercation resulted in the discharge of a firearm by a police officer, it rose to the level of a "critical incident" per the CPRA, giving the City the discretion to determine whether or not to use redaction technology to protect the identities of certain individuals in the recording.[30] Given that those seeking care at a Planned Parenthood facility have a reasonable expectation of privacy, and given that the visitors to Planned Parenthood had no relation to the altercation in question, the City decides it will blur out the faces of those people unrelated to the altercation.

---

[29] California Attorney General's Office, *Summary of the California Public Records Act 2004*, at 7, http://ag.ca.gov/publications/summary_public_records_act.pdf (last visited Apr. 26, 2019).
[30] Cal. Gov't Code § 6254(f)(4)(B)(i)–(ii).

The City leaves all other parts of the footage intact and discloses the partially redacted video recording to the reporter.

Example #3: Promoting Security through Disclosure

The City recently launched a new interface for submitting job applications to the City. Unfortunately, it just discovered a major security vulnerability that would allow an attacker to bypass authentication and access sensitive personnel files maintained on a related webpage by the Human Resources Management Department. The vulnerability could take weeks to patch, and it currently remains exploitable. Meanwhile, a curious IT professional, submits a CPRA request to the City of Oakland seeking information about its public website, www.oaklandca.gov, including the new job application interface.

The City locates the relevant records, but realizes they include very recent emails between members of the IT Department discussing the details of the vulnerability. The City Attorney's Office immediately seeks guidance from the IT Department about how to proceed, since it knows this request might pose some privacy and security concerns. Disclosure of these records could put the City at serious risk of malicious hacking. Moreover, exploitation of this particular vulnerability could result in the leaking of very sensitive City personnel information. Accordingly, the IT Department and the City Attorney's Office jointly decide that the City must not disclose specific portions of emails that would allow a malicious actor to exploit the vulnerability until the City can address it.

BE TRANSPARENT AND OPEN

Oaklanders' right to privacy is furthered by the ability to access and understand explanations of why and how we collect, use, manage, and share personal information. To that end, we aim to communicate these explanations to Oakland communities in plain, accessible language on the City of Oakland website. We also aim to communicate this information at a time when it is relevant and useful.

I. Purpose and Goals of the Transparency Principle

The Transparency Principle intends to establish trust between the City of Oakland and its residents by informing them about City privacy practices in a way accessible to them. Increased openness builds trust and facilitates citizen engagement in deliberations on privacy issues. Transparency and openness are ongoing commitments to provide regular information as privacy practices change and adapt in the face of evolving technology.

The Transparency Principle is grounded in various state and municipal laws, including the Ralph M. Brown Act,[31] the Oakland Sunshine Ordinance,[32] the Privacy Advisory Commission ("**PAC**") Ordinance,[33] and the Oakland Surveillance and Community Safety Ordinance (**"Surveillance Ordinance"**).[34] The Brown Act and Sunshine Ordinance's requirements of regular order and public availability of meeting and hearing documents reflect the view shared at the state and local level that transparency and openness are essential to effective democratic governance. The PAC Ordinance and the Surveillance Ordinance similarly make good on the City's commitment to transparency regarding matters of city administration when it comes to the growing role that technology plays in the collection of personal information. Nothing in the Transparency Principle limits the application of these state and municipal laws. Rather, the Transparency Principle intends to communicate to Oaklanders, when possible, the information security practices undertaken by the City to protect individual privacy.

The Transparency Principle also emphasizes the City's commitment to communicate relevant information to all Oakland communities in "plain, accessible language." Plain language increases the clarity of information about privacy practices. "Accessible language" means providing information in multiple languages and in formats useful to the blind and print disabled. The Principle's accessibility provision is grounded in state and local ordinances. The California Civil Rights Act and The Bilingual Services Act are the two main state statutes governing language access services.[35] Both mandate that local agencies provide language access services to individuals with

---

[31] *See* Cal. Gov't Code §§ 54950–63.
[32] *See* Oakland, Cal., Ordinance 11957 (1997); Oakland, Cal., Ordinance 12483 (2003).
[33] *See* Oakland, Cal., Ordinance 13349 § 2(a)–(b).
[34] *See* Oakland, Cal., Oakland Surveillance and Community Safety Ordinance §§ 9.64.010(6)–(7); § 9.64.020; § 9.64.030(3).
[35] *See* Cal. Gov't Code § 11135(a); Cal. Gov't. Code § 7290.

limited proficiency in English. Oakland was the first city in the U.S. to implement a language access ordinance as the "Equal Access to Services Ordinance,"[36] expanding definitions and providing specific guidance to fulfill obligations under the California Bilingual Services Act.[37]

II. Examples Illustrating the Transparency Principle in Practice

Example #1: Homelessness and Housing Units

An employee at the Department of Housing and Community Development wants to help develop more low-income housing projects in Oakland. The project requires her team to gather data and create reports about homelessness in the City. Over the course of the project, the team plans to conduct surveys at various homeless shelters, with the intent to gather residents' personal information including names, dates of birth, employment information, and mental health history. The Department wants to emphasize to potential participants that while the survey is entirely optional, it provides valuable information that can be used to better serve Oakland residents.

The Department proactively informs individuals about purpose of the survey, the information collected, any other departments that may be able to access the information, and the option to not participate. It also posts notices regarding the project both online and in shelters in multiple languages. The notice is simply worded and provided in formats accessible to print disabled residents.

Example #2: Public Works and Rain Barrel Project

An employee for the Oakland Public Works Department wants to build on the success of the last Oakland Rain Barrel Program to better conserve resources and protect the Oakland environment by recycling rainwater. As part of the project, the City is required to survey homes that might have the capability to install rain barrels safely so it can determine a working budget to subsidize the cost. The City plans to collect residents' names, addresses, household size, water usage patterns, and interest in the program in order to determine contract requirements for local installers of the rain barrels.

Recognizing the significant amount of personal information being collected for implementation of the project, the Public Works Department decides to inform Oakland residents about the types of personal information collected in the survey. The City includes this information in flyers about the program, which also includes contact information and link to the Department's webpage, in multiple languages.

[36] *See* Oakland, Cal., Mun. Code § 2.30.
[37] *See* Oakland, Cal., Mun. Code, § 2.30.020(d).

Example #3: Department of Transportation/Oakland Police Department Intersection Danger

A particular neighborhood intersection has been the site of numerous accidents, some of which have been fatal. The Department of Transportation ("**DOT**") and the Oakland Police Department ("**OPD**") confer and decide that installing a traffic camera at that intersection would help reduce the number of accidents. They present their plan to add cameras to the intersection at the monthly PAC meeting, which approves the installation after hearing members of that neighborhood advocate in support of the camera installation. However, some neighborhood advocates are concerned that the camera might also surreptitiously monitor the activity of individuals near the intersection in non-traffic related incidents.

Acknowledging the importance of this concern raised by some members of the community, the departments decide to notify neighborhood residents about the installation of the camera, the purpose and limitations of data analysis, and any additional privacy precautions that the PAC advises such as drawing attention to the cameras themselves with highly visible notices. Since the primary language in this community is not English, the notices posted around the neighborhood are translated into multiple languages. The notice also appears on both the DOT and OPD websites.

BE ACCOUNTABLE TO OAKLANDERS

Trust in our stewardship of personal information requires both that we collect and manage personal information appropriately, and that we create opportunities for active public participation. We publicly review and discuss departmental requests to acquire and use technology that can be used for surveillance purposes. We encourage Oaklanders to share their concerns and views about any system or department that collects and uses their personal information, or has the potential to do so. We also encourage Oaklanders to share their views on our compliance with these Principles.

I. Purpose and Goals of Accountability Principle

The Accountability Principle ensures that the City of Oakland is answerable to its residents when it collects and manages their personal information by proactively seeking input through legislative and administrative bodies such as the Privacy Advisory Commission ("**PAC**") about the City's compliance. The Accountability Principle emphasizes the importance of giving Oakland residents whose privacy interests may be impacted by city policies information about those policies and an opportunity to weigh in on them. The Principle acknowledges that accountability requires more than serving as a passive receptacle for feedback. The goal of the Principle is to lower barriers for civic participation on questions of privacy. By soliciting feedback from a wide and diverse pool of residents, the City can safeguard the privacy and security of all residents, especially marginalized communities who are most affected by inequitable data collection practices and may face barriers to participating in the decisionmaking process.

The Accountability Principle also calls for residents' views on compliance with the Principles themselves. Because of constantly changing technology and the increasing sophistication of residents' conception of their privacy rights, the precise steps the City must take to meet the standards set by the Principles may evolve over time. By asking for feedback on compliance with the Principles, the City can continue to refine its approach to privacy in a democratic and participatory manner.

PAC provides a model for this kind of engagement. Because PAC conducts monthly meetings and uses other public forums to collect and receive public input, Oaklanders have the opportunity to weigh in on any surveillance technology that can collect residents' personal information.[38] PAC also makes publicly available City departments' annual use reports, privacy analyses, and data retention policy recommendations regarding the City's deployment of existing and proposed surveillance equipment and technologies.[39]

---

[38] *See* Oakland, Cal., Ordinance 13,349 § 2(b).

[39] *See* Oakland, Cal., Ordinance 13,349 § 2(e)–(g); Oakland, Cal., Oakland Surveillance and Community Safety Ordinance §§ 9.64.010(6), (7), 9.64.020, 9.64.030(3).

II. Examples Illustrating the Accountability Principle in Practice

Example #1: Parks Department Privacy Training

An Oaklander volunteering at the Lakeview Park Kitchen Garden is surveyed by some Parks, Recreation & Youth Development Department employees as part of a research project. The employees ask for Oakland residents' name, age, district affiliation, and information about what times they go to parks and which parks are closest to their homes. Although the volunteer agrees to participate in the survey, she is concerned about the amount of personal information being collected by the Department.

After finishing her shift at the Kitchen Garden, the volunteer decides to email the Director of the Department to let him know about her concerns with the Department's survey practices and the amount of information collected on her. The Director of the Parks Department, who is aware of the Oakland Privacy Principles, responds to her and also decides to flag the information for the City's Chief Privacy Officer to review compliance with the Privacy Principles. The Privacy Officer reviews the survey practices and communicates to the Department necessary guidance on how to best comply with the Principles. The Parks Department sends a follow-up note to the resident who flagged the concern.

Example #2: Automated License Plate Reader Hearing at PAC

An Oakland resident learns that the Department of Transportation has been using Automated License Plate Readers ("**ALPR**") to enforce parking regulations. She finds the use of ALPR invasive and worries that the same vehicle has captured her information on multiple occasions.

To voice her concerns in a public forum, she decides to attend an upcoming PAC meeting where the Department's use of ALPR is being considered. After hearing PAC's deliberative process and department officials speaking in support of ALPRs, the resident lays out her concerns about how her image and information has been captured by the ALPR repeatedly. Hearing her account, PAC recommends adjusting the angle of the ALPR camera to limit capture of driver images going forward, leading to amendments to the ALPR Surveillance Use Policy.

Example #3: Air Quality Surveys

The Oakland High School Environmental Science Academy team is participating in a community project measuring the disparity in air quality in different areas of Oakland. The team is tasked with collecting health information on the individuals living in areas near the devices. They want to test whether there is a correlation between areas with higher particulate matter in the air and increased incidences of asthma and chronic obstructive pulmonary diseases in the local population groups. This involves surveying local populations about personal information, including names, genders, ages, and medical history. The City is also very interested in the results of the team's research.

Recognizing the sensitive nature of the information collected as well as the City's responsibility to protect Oaklanders' privacy and information security, the City decides to include language to proactively inform all survey participants of the purpose of the data being collected as well as contact information for a privacy officer for the Oakland Unified School District so that participants can give any feedback on any concerns they might have about the data collection or the District's compliance with the Privacy Principles.

CONCLUSION

Collectively, the Privacy Principles create a citywide standard for privacy practices in Oakland. This Guidance document illustrates how City departments should apply the Principles in practice. While the Principles express Oakland's privacy values, the Guidance helps to harmonize the ways different City departments—from the Oakland Police Department to the Department of Public Works to IT—use the Principles to protect Oaklanders' privacy interests in the course of providing city services. This Guidance is a living document and will be updated periodically to respond to changes in information technology and evolving norms and understandings of privacy, information security, and civil liberties.

If you have any questions or concerns about any aspects of the Principles or this accompanying Guidance, we encourage you to reach out to the Oakland Privacy Advisory Commission ("**PAC**") directly or to participate in a monthly PAC meeting to share your insights or seek more information.

CITY OF OAKLAND

MEMORANDUM

TO: Privacy Advisory Commission

FROM: Anne E. Kirkpatrick, Chief of Police

SUBJECT: OPD – FBI 2018 Joint Terrorism Taskforce (JTTF) Annual Report

DATE: April 22, 2019

EXECUTIVE SUMMARY

Ordinance No. 13457 C.M.S. approved by the City Council on October 3, 2017, adds Chapter 9.72.010 to the City of Oakland Municipal Code (OMC) concerning "Law Enforcement Surveillance Operations." OMC 9.72.010 requires that, among other requirements, that by January 31 of each year, the Chief of Police shall provide to the Privacy Advisory Commission and City Council, a public report with appropriate public information on the Police Department's work with the JTTF or other federal law enforcement agency task force in the prior calendar year. OPD has already introduced a draft 2018 FBI JTTF Taskforce annual report to the PAC at its February ; this report provides updated information for 2018.

STAFFING, EQUIPMENT AND FUNDING

As of January 1, 2018, one employee (sworn OPD Officer) was assigned to the FBI Joint Terrorism Task Force. The Officer was assigned to work a standard regular work week of (40) forty hours per week. This Officer is assigned to OPD's Intelligence Unit and has a joint duty of also participating and assisting with the FBI JTTF. The Officer's duties and reporting responsibilities depend upon whether there is any active counter-terrorism investigation as well as the current needs and priorities of the OPD Intelligence Unit.

The position is compensated as a regular OPD Officer; the FBI does not compensate OPD for this position's salary. The Officer position works regular hours: 40 hours per week; 1,920 hours per year (approximately). Any overtime (OT) hours specific to taskforce operations are paid by the FBI - in 2018, the OPD JTTF did not work any OT hours related to JTTF duties.

In 2018, the JTTF Officer was on special loan from the Intelligence Unit and assigned to the Bureau of Services for all of 2018; this Officer only participated minimally in JTTF operations (approximately 1-2 times a month). However, as the JTTF Officer continues to be a member of the Task Force, the FBI provided a vehicle, covered all fuel expenditures and allowed access to the FBI JTTF office space and access to FBI data systems.

CASES ASSIGNED TO THE OPD JTTF OFFICER

In 2018, the OPD JTTF Officer was on special loan to the Bureau of Services (ongoing), and was not assigned to any JTTF Task Force cases as a lead investigator. The OPD JTTF Officer does not manage any informant relationships. The Task Force Officer has assisted in JTTF investigations. An example of this support is the October 2018 pipe bomb investigation in which Bay Area

politicians and members of the media received pipe bombs in the mail. OPD was concerned that local figures in Oakland were also targeted. The OPD JTTF Officer coordinated with the Task Force on investigations (the Task Force determined that no Oakland based officials were targeted, and this information was relayed to City officials). Another Task Force-related case involves the 2016 FBI arrest of Amer Alhaggagi. The investigation revealed that Alhaggagi planned to: set fires in the hills of Berkeley, strategically place backpack bombs in various public areas around downtown Oakland, sell cocaine laced with rat poison at bars and clubs in Oakland and Berkeley, and detonate a car bomb at a gay nightclub in San Francisco. The FBI learned that in July of 2016, Alhaggagi had applied to the Oakland Police Department for a position as a police Officer. The Oakland JTTF Officer assisted the FBI in identifying Alhagaggi as the subject. Ultimately, the FBI was able to safely arrest him. Alhaggagi was sentenced to 15.5 years' imprisonment because of his conviction on the above mentioned criminal activity.

UNDERCOVER OPERATIONS AND INTERVIEWS

In 2018, the OPD JTTF Officer did not conduct any undercover operations or interviews (JTTF interviews are normally conducted by FBI Agents). In 2018, the OPD JTTF Officer did not take part in any interviews (voluntary or involuntary).

The FBI is aware of requirements mandated of OPD and its protocols for undercover operations and interviews; the Task Force Officer was always held responsible for following all sworn Officer policies and standards.

TRAINING AND COMPLIANCE

The OPD JTTF Officer follows all OPD policies and receives several police trainings, including but not limited to: continual professional training, procedural justice, and annual firearms training. The Officer has also reviewed all provisions of the JTTF MOU. The JTTF Officer as well as supervisor are held responsible by OPD for compliance with all applicable Oakland and California laws.

The OPD JTTF Officer supervisor (Intel Sergeant) conducts mandatory bi-weekly meetings with the officer. Daily and weekly meetings are also held when critical incidents occur.

ACTUAL AND POTENTIAL VIOLATIONS OF LOCAL/STATE LAW

The JTTF OPD Officer had no violations of local, California, or Federal law. OPD Command consults with the Office of the City Attorney to ensure that all polices conform with State and Federal laws.

SUSPICIOUS ACTIVITY REPORTING (SARs) and NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER (NCRIC)

OPD submits Suspicious Activity Reports (SARs) to the Northern California Regional Intelligence Center (NCRIC). These reports contain information regarding activity, such as, but not limited to: narcotics, cyber-attacks, sabotage, terrorism threats, officer safety, and human trafficking. NCRIC provides a secure online portal where police agencies can provide this information. NCRIC has shared with OPD that providing false or misleading information to NCRIC is a violation of Federal Law and may be subject to prosecution under Title 18 USC 1001. The JTTF is a recipient of SAR

information. The OPD JTTF Officer submitted zero SARs to NCRIC during the 2018 calendar year. It is unknown how many SAR's OPD Officers received during 2018.

COMMAND STRUCTURE FOR OPD JTTF OFFICER

The OPD JTTF Officer works under the command structure of OPD; the OPD JTTF Officer reports directly to the OPD Intelligence Unit Supervisor (Sergeant). The Officer also coordinates with the FBI Supervisor, who is also serves as a Counterterrorism Assistant Agent.

Respectfully submitted,

Anne E. Kirkpatrick,
Chief of Police

Reviewed:
Bruce Stoffmacher, Acting Police Services Manager
OPD, Research and Planning Unit, Training Division

Prepared by:
Omar Daza-Quiroz, Sergeant of Police
OPD, Intelligence Unit

Proposed Amendment to Chapter 9.64 Regulations on City's Acquisition and Use of Surveillance Technology

Definition (Muni Code Section 9.64.010 Definitions):

13. "Face Recognition Technology" means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face.

Operative language (Muni Code Section 9.64.030 City Council approval requirements for new and existing surveillance technology):

(F) Notwithstanding any other provision of this Section, it shall be unlawful for any City staff to obtain, retain, request, access, or use: 1) any Face Recognition Technology; or 2) any information obtained from Face Recognition Technology. City staff's inadvertent or unintentional receipt, access to, or use of any information obtained from Face Recognition Technology shall not be a violation of this subsection (F), provided that:

(1) City staff does not request or solicit its receipt, access to, or use of such information; and

(2) City staff logs such receipt, access to, or use in its Annual Surveillance Report.

APPROVED AS TO FORM AND LEGALITY

CITY ATTORNEY'S OFFICE

AMENDED AT THE APRIL 24, 2018 PUBLIC SAFETY COMMITTEE

OAKLAND CITY COUNCIL

ORDINANCE NO. 13489 C.M.S.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:

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

hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each Police Area in the relevant year;
E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties.
F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.
G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

2. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.

3. "City staff" means City personnel authorized by the City Administrator or designee to seek City Council Approval of Surveillance Technology in conformance with this Chapter.

4. "Continuing agreement" means an agreement that automatically renews unless terminated by one party.

5. "Exigent circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

6. "Large-scale event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.

7. "Personal communication device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.

8. "Police area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

9. "Surveillance" or "surveil" means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by license plate data when combined with any other record.

10. "Surveillance technology" means any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.

    A. "Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

1. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used for any surveillance or law enforcement functions;
2. Parking Ticket Devices (PTDs);
3. Manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings;
4. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;
5. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;
6. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.
7. Medical equipment used to diagnose, treat, or prevent disease or injury.
8. Police department interview room cameras.
9. Police department case management systems.
10. Police department early warning systems.
11. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above.

6. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

   A. **Description:** Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
   B. **Purpose:** Information on the proposed purposes(s) for the surveillance technology;
   C. **Location:** The location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
   D. **Impact:** An assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

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

7. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

A. **Purpose:** The specific purpose(s) that the surveillance technology is intended to advance;
B. **Authorized Use:** The specific uses that are authorized, and the rules and processes required prior to such use;

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

9.64.020 Privacy Advisory Commission (PAC) Notification and Review Requirements

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

A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:

1. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,
2. Soliciting proposals with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.

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

C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020.1.B, City staff may proceed and seek Council Approval of the proposed Surveillance Technology initiative pursuant to the requirements of Section 9.64.030.

2. PAC Review Required for New Surveillance Technology Before City Council Approval

A. Prior to seeking City Council approval under Section 9.64.030, City staff shall submit a Surveillance Impact Report and a Surveillance Use Policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to City staff. City staff shall present such

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

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval

A. Prior to seeking City Council approval for existing City surveillance technology under Section 9.64.030 City staff shall submit a Surveillance Impact Report and Surveillance Use Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under 9.64.010.

B. Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, City staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the City.

C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.

D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020.1.C., City staff shall submit at least one (1) Surveillance Impact Report and proposed Surveillance Use Policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable City staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

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

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

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

2. City Council Approval Process

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

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

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

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

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

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

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

9.64.040. Oversight Following City Council Approval

1. On March 15th of each year, or at the next closest regularly scheduled Privacy Advisory Commission meeting, City staff must present a written Annual Surveillance Report for Privacy Advisory Commission review for each approved surveillance technology item. If City staff is unable to meet the March 15th deadline, City staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.

   A. After review by the Privacy Advisory Commission, City staff shall submit the Annual Surveillance Report to the City Council.

   B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the corresponding Surveillance Use Policy that will resolve the concerns.

   C. Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the Annual Surveillance Report.

   D. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 9.64.030 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval.

2. Based upon information provided in City staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory

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

9.64.050. Enforcement

1. Violations of this article are subject to the following remedies:

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

9.64.060. Secrecy of Surveillance Technology

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

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

9.64.070. Whistleblower Protections.

1. Neither the City nor anyone acting on behalf of the City may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:

   A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; or
   B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Ordinance.

2. It shall be grounds for disciplinary action for a City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any Surveillance Use Policy or Administrative Instruction promulgated under this Ordinance.
3. Any employee or applicant who is injured by a violation of this section may institute a proceeding for monetary damages and injunctive relief against the City in any court of competent jurisdiction.

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

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

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

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

IN COUNCIL, OAKLAND, CALIFORNIA, MAY 15 2018

PASSED BY THE FOLLOWING VOTE:

AYES - BROOKS, CAMPBELL-WASHINGTON, GALLO, GIBSON MCELHANEY, GUILLÉN, KALB, KAPLAN - 7
AND PRESIDENT REID

NOES - Ø

ABSENT - Ø

ABSTENTION - Ø

1 Excused - Reid

Introduction Date

MAY 01 2018

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

Date of Attestation: May 18, 2018

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report for Remote and Live-Stream ~~Mobile~~ Camera Systems~~s~~

1. Information Describing Remote and Live-Stream~~Mobile~~ Camera Systems (RLSC)~~s~~ and How They Work

OPD utilizes different types of cameras to capture single image and video data. Cameras that are strictly manually operated are not considered "surveillance technology" under the Oakland Surveillance Ordinance No. 13489 C.M.S. However, some cameras ~~RMCs~~ allow for remote access and/or live-streaming~~real-time remote access viewing~~ of activity. ~~captured by the RMC lens.~~ Single image and video cameras~~RMC~~s may be manufactured with data transmitting technology or be outfitted by OPD with separate camera transmitters. Remote-control functions allow personnel to observe and/or record activity without being near potentially dangerous situations. Live-stream access allows personnel to observe situations in real-time and have the option to respond immediately when situations require immediate response. Remote~~Mobile~~ functionality allows cameras~~RMCs~~ to be moved and positioned as the need requires.

RMCs may have their own power supply or attached to a utility pole so as to utilize electricity for power. In either case, RLSCs~~RMCs~~ offer personnel critical situational and evidentiary information in a safe way.

RLSC~~MC~~s store visual (and sometimes audio) data with either internal storage and/or by transmitting data in real-time to a remote OPD location.

2. Proposed Purpose

RMCs are used by OPD authorized personnel to gather evidence during undercover operations as well as during large events where there is a greater probability that criminal activity may occur and public safety is more likely to be impacted; the City's Surveillance Technology Ordinance[1] ~~defines~~ "large-scale event(s)" as events "attract(ing) ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur." OPD may also use live stream cameras on poles held by officers to observe smaller events in the scores or hundreds of people where the same conditions exist.

[1] Ordinance No. 13489C.M.S. passed by the City Council on May 15, 2018

~~mass-events personnel are deployed to observe and promote public safety.~~ Live stream image and video capture allow investigators to observe activity related to suspected criminal activity.

3. Locations Where, and Situations in which RLSCs~~GLD System~~ may be deployed or utilized.

A RLSC~~MC~~ may be used anywhere in the public right of way within the City of Oakland. Personnel may use hand-held cameras with live-viewing capabilities within in the public right of way within the City of Oakland; however, these cameras are generally only used for mass-person events to as to provide situational awareness during events where public safety must be monitored (e.g. large protests or parades). OPD ~~RMCs~~ may also request that a utility company install a remote camera ~~RMC to a~~on an electricity utility pole for powered live-remote viewing. OPD will only request to install a such a camera ~~RMC~~ to a utility pole with a court order compelling ~~allowing~~ the utility company to install the camera.

4. Impact

RLSC~~MC~~s offer evidentiary and situational awareness in numerous ways that challenge measurement. Mass events where thousands of people gather require that police personnel see where people are moving in real-time to better ensure that resources are provided as needed to ensure public safety.

OPD's Criminal Investigations Division (CID) and Intel Unit occasionally need to monitor street locations with remote live-view cameras to gather evidence related to suspects in criminal cases. RLSC~~MC~~s can provide useful evidence about particular suspects relating to violent criminal activity.

OPD recognizes that any use of cameras to record activity which occurs in the public right of way raises privacy concerns. There is concern that the use of RMCs can be utilized to identify the activity, behavior, and/or travel patterns of random individuals. However, OPD does not randomly employ this technology throughout the City. Rather, RLS~~M~~Cs installed on utility poles (after obtaining a court order) are used in specific situations to gather evidence about particular individuals connected to particular criminal investigations. The scope and use of such technology is narrow and limited. Therefore, OPD believes that the impact to public privacy is similarly narrow and limited.

5. Mitigations

All live-stream cameras ~~RMCs~~ shall be housed and secured within ~~IT~~ OPD's IT Unit ~~or Intel Unit~~ lockers and not accessible with to the public or to personnel

without permission to use such equipment. Regular camera data from live-stream cameras shall be uploaded onto a secure computer with user and email password protection. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Otherwise, camera data will be destroyed after 30 days.

OPD does not possess remote cameras which are affixed to utility poles. Rather, OPD relies on its partnership with the Bureau of Alcohol, Tobacco, and Firearms (ATF) through the ATF Taskforce to directly install remote cameras, when approved by a judge in a court order, as part of a documented investigation (ATF personnel install and de-install the camera equipment). Generally, each request to install a remote camera to a utility pole is connected violent criminal activity (gun crimes, homicides, gun sales and/or major narcotic traffic activity).

~~OPD will consider providing RMC data to other law enforcement (LE) agencies if and when such agencies make a written request for the RMC data that includes:~~

~~a. The name of the requesting agency.~~
~~b. The name of the individual making the request.~~
~~c. The intended purpose of obtaining the information.~~

~~Such requests will be reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled. Approval requests shall be retained on file. Requests for RMC data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public Records Access (Civil Code § 1798.90.55) and per any interagency agreements.~~

OPD will monitor its use of RLSC~~MC~~s to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits. ~~-~~The IT Unit ~~RMC System~~ Coordinator and/or designated staff shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains following for the previous 12-month period following a reporting structure agreed upon by the Privacy Advisory Commission.

6. Data Types and Sources

RLS~~M~~Cs that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.

RLS~~M~~Cs can be mounted to telescoping monopods to simply extend the range of a RLS~~M~~C. In these instances the pole merely extends the reach of the camera. RMCs mounted to monopods operate similarly to other RMCs in terms of recording and storage functions.

Cameras~~RMCs~~ may be connected to a transmitter which allows for real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

7. Data Security

All RMCs shall be housed and secured within IT Unit or Intel Unit lockers and not accessible with to the public or to personnel without permission to use such equipment. Regular camera data shall be uploaded onto secure computer with user and email password protection. For data that is captured and used as evidence, such data shall be turned in and stored as evidence. Otherwise, camera data will be destroyed after 30 days.

Judges approve remote cameras to be affixed to utility poles to record public right of way views for 30 days or less (90 days maximum). OPD archives video sections relevant to investigation (permanent retention) and deletes other non-evidentiary video footage.

8. Costs

OPD currently has owns four transmitters from TVU networks that allow standard single shot or video cameras to live-stream data to OPD's Administration Building or the City's Emergency Operations Center (this data is not recorded). These transmitters are approximately eight years old. OPD does not currently pay for ongoing maintenance service; the cost to upgrade the unsupported system would cost about $120,000 for a two-year maintenance contract and then $12,000 for additional years. OPD is planning to use approximately $130,000 from the Justice Assistance Grant (JAG) Program[2] to pay four new modern TVU Networks transmitters. OPD does not bear costs related to ATF remote camera installations.
~~TBD~~

9. Third Party Dependence

OPD uses TVU Networks-brand transmitter for live-stream video camera monitoring. ~~TBD~~OPD relies on the ATF to install remote cameras to utility

[2] https://www.bja.gov/jag/

poles (with court order approval).

10. Alternatives Considered

OPD officers and personnel rely primarily on traditional policing techniques to monitor large events and to gather evidence related to criminal investigations. For decades evidence gathering also includes the use of cameras, sometimes with live-stream transmitters, to record images, video and audio. Police personnel must maintain some level of situational awareness when hundreds and thousands of people gather on public streets and threats to public safety increase. Alternatives to live-stream ~~camersa~~cameras would include having more officers and personnel deployed during every mass-event. Such a deployment extends beyond OPD budget capacity.

OPD relies on remote view cameras for investigations as described above. There is no clear alternative to capturing actionable image, video and/or audio.

11. Track Record of Other Entities

There is no well documented public record of RLSCs. However, a recent case concerning remote cameras illustrates legal considerations: the Tenth Circuit Court of Appeals decided in "*United States v. Cantu[i]"* (October 2017) in which the court discussed whether the use of a utility pole camera that viewed the front of Cantu's residence violated his rights under the Fourth Amendment[3]. The relevant facts of Cantu, taken directly from the case, are as follows: ~~TBD~~ On appeal, the issue was whether the warrantless use of camera on a utility pole that viewed the front of his residence (public right of way) violated rights under the Fourth Amendment. The Court in *Cantu* noted that the police did not install the camera on Cantu's property, thus there was no trespass; Also, the Court concluded that Cantu did not have a reasonable expectation of privacy where he was walking with the rifle.

Formatted: Font color: Custom Color(RGB(34,34,34)), Pattern: Clear (White)

[3] https://www.llrmi.com/articles/legal_update/2017_united_states_v_cantu/

DEPARTMENTAL GENERAL ORDER

##: REMOTE OR LIVE-STREAM~~AND~~ CAMERAS (RLSC)

Effective Date: ~~XX Apr 19~~
Coordinator: Information Technology Unit, Bureau of Services Division

The Oakland Police Department (OPD) uses technology to more effectively promote public safety; OPD also strives to institute policies that promote accountability and transparency. This policy provides guidance and procedure for the use, documentation, and auditing of live-stream mobile cameras.

All data, whether sound, image, or video data, generated by different types of camera recording technology are ~~OPD's~~ RLSC ~~systems are~~ for the official use of this department. Because such data may contain confidential information, such data is not open to public review.

A. Purpose of the Technology

A – 1. Authorized Use

There are different situations that can occur in the City of Oakland which will justify the use of live-stream cameras and/or remote control cameras that may record and/or allow for live streaming from remote locations. Large events with numerous people (e.g. protests, sporting events, parades, large festivals) can attract individuals seeking to engage in violent criminal behavior and/or large-scale property destruction. Authorized personnel utilizing cameras with live-streaming transmitters can provide important situational awareness to OPD; OPD can better respond to sudden dangerous activity (e.g. aggravated assault) with this remote situational awareness.

Formatted: Indent: First line: 0"

Specific criminal investigations also benefit from remote-functioning cameras that record the public right of way in particular locations where serious criminal activity occur is believed to occur.

Formatted: Indent: Left: 0.49", Right: 0.29", Space After: 6 pt

Personnel authorized to use RLSCs or access information collected through the use of such equipment shall be specifically trained in such technology and authorized by the Chief of Police or designee. Any sworn officer may utilize hand-held live-stream cameras with the approval of OPD's Information Technology (IT) Unit Coordinator. Remote cameras installed to utility poles for remote power and use may only be employed by any OPD by first receiving: 1) a court order from a judge authorizing the restricted camera use in a specific location for a specified number of days; and 2) the OPD Intel Unit Supervisor.

~~uch personnel shall be limited to designated captains, lieutenants, sergeants, officers, police service and/or evidence technicians, and crime analysts unless otherwise authorized.~~

A – 2. Prohibited Use

1. Department members shall not use, or allow others to use RLS~~M~~C equipment, software or data for any unauthorized purpose.

~~No member of this department shall operate~~ RLSC ~~equipment or access the internally stored~~ RLSC ~~data without first completing department-approved training.~~

2. The RLS~~M~~C systems shall only be used for official law enforcement purposes. No OPD personnel is authorized to install cameras to utility poles; personnel shall coordinate utility pole camera installation with third-party partners (such as the Bureau of Alchohol Tobacco and Firearms (ATF)) after receiving Intel Unit Supervisor approval as well as a court order from a judge.

3. Only specifically authorized personnel authorized by the Chief or Chief-designee (e.g. personnel with OPD's IT ~~nformation Technology~~ Unit and Criminal Investigations Division (CID) investigators, Internal Affairs Division personnel, crime analysts, the Office of the District Attorney) will have access to RLS~~M~~C audio and video data and system applications.

4. Accessing data collected by RLS~~M~~C systems requires a right to know and a need to know. 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 criminal or administrative investigation.

B. Description of the Technology

B– 1. General Description of Remote or Live Stream Cameras

~~**A – 1. How Remote and Mobile Cameras (RLSC) Work**~~

RLSCs can be self-contained devices that record audio and video, which either: 1) store data onto an internal storage device; or 2) transmit data in real-time through various digital transmission formats.

1. RLSCs that record directly onto an internal memory device (e.g. secure digital (SD) card) operate similar to consumer digital video cameras. These types of cameras contain an internal storage device for storing audio and video data – an integrated element that can be connected to a computer for data downloads, or a removable device (e.g. SD card) which can be connected to a computer for digital downloads.
2. RLSCs can be mounted to telescoping monopods to simply extend the range

Formatted: Indent: Left: 0.5", Hanging: 0.25"

Formatted: No bullets or numbering

Formatted: Indent: Left: 0.5", Hanging: 0.25"

Formatted: List Paragraph, Right: 0", Space After: 6 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.5", Hanging: 0.25"

of a RLSC. In these instances the pole merely extends the reach of the camera. RLSCs mounted to monopods operate similarly to other RLSCs in terms of recording and storage functions.

3. RLSCs may be connected to a transmitter which allows for real-time transmission and remote live-stream viewing. Transmitters can use different formats (e.g. cellular 3G/4G LTE, WiFi, Ethernet, and Microwave). Transmitters can be connected to static single image digital cameras or video cameras. Transmitters allow the live-stream images or video to be viewed on a screen with the appropriate data connection and reception technology. The transmitters specifically transmit the data to a receiver where the data can then be viewed.

B– 2.How Cellular Remote or Live-Stream Cameras WorkRLSC

Live-stream transmitters can be attached to ~~Some RLSCs are~~ standard consumer-type cameras ~~that that can be held and operated by personnel~~so that images and/or video can be transmitted. These RLSCs ~~may also be affixed to a variable lens's for different views. RLSCs~~ can be attached to a camera monopod and used like a standard digital video camera; the monopod in this case extends the cameras perspective beyond arms ~~–~~reach so that personnel extend the range of view (beyond corners, above head-level in a crowd, or in other related situations). RLSCs attached to monopods/tripods provide greater viewing access and promote safety where personnel may need to exercise caution before moving into unknown situations.

Some cameras~~RLSCs~~ may also be attached to utility poles for real-time and long-term remote viewing. In such cases RLSCs may be powered through electricity of the utility pole or via portable battery power. In either case, RLSCs offer personnel critical situational and evidentiary information in a safe way.

C. ~~C.~~ RLSCRLSC Data Collection

C – 1. Live-Stream Camera Information Collected
~~Data Collection and Retention~~

Live-stream camera ~~RLSC system~~ data is maintained by ~~both by currently maintained by either: 1)~~ the OPD ~~Information Technology (~~IT~~)~~ Unit within in the Bureau of Services (BOS)~~; or 2) by the Intel Unit~~. Personnel using live-stream cameras (cameras with attached transmitters) ~~RLSCs from the Intel Unit sh~~shall return RLSCs at the end of their shift to the IT Unit. The IT~~Intel~~ Unit RLSC Coordinator shall download the data onto secure IT~~ntel~~ Unit computer~~s~~ within 24 hours of receiving returned RLSC equipment.

The IT~~ntel~~ Unit shall maintain all RLSC data for 30 days unless notified by the Chief of Police or designee (e.g. Internal Affairs Captain or Criminal Investigations personnel) that the image and video data is needed for an

Formatted: Indent: Left: 0"

Formatted: Space After: 6 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5", Widow/Orphan control

Formatted: Indent: Left: 0.49", First line: 0", Right: 0.29"

investigation. The IT ~~OPD~~ Unit RLSC Coordinator ~~and/or assigned personnel issued the RLSC~~ is responsible for recovering the data from the RLSC.

Data that is part of an investigation shall be provided to the appropriate personnel as a separate digital data file, kept permanently as part of the official investigation record.

The IT Unit shall delete all RLSC data left on installed on IT Unit computers after 30 days unless otherwise notified to maintain the data as part of an investigation as detailed above.

C – 2. Remote Camera Information Collected

The Intel Unit is responsible for the use and coordination of remote cameras attached to utility poles for remote power, use and viewing. The Intel Unit is authorized to participate with the ATF and/or other approved taskforce partners on the installation of remote cameras. The ATF and/or other approved taskforce partner will be responsible for the collection of pole camera image and video data. Only image and video data needed for lawful police investiagtions and for evidence shall be maintained indefinitely by OPD; the Intel Unit shall be responsible for maintain this data.

C – 3. Limitations on Information Collected

Remote pole camera image and video data shall only be generated with the approval of a judge's court order; a pole camera may only be used during the allowed recording period, which is usually 30 days or less, and generally never more than 60 days.

C – 4. Monitoring and Reporting

The Oakland Police Department will monitor its use of the RLSC system to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process, and time period system audits.

The IT Coordinator, Intel Unit Coordinator, or other designated OPD personnel shall provide the Chief of Police, Privacy Advisory Commission, and City Council ~~Public Safety Committee~~ with an annual report that contains following for the previous 12-month period:

1. The number of times a RLSC was deployed, and type of deployment.
2. The number of times RLSC data was used as part of an investigation.
2. A list of agencies other than OPD that were authorized to use the equipment.
3. A list of agencies other than the OPD that received information from use of

Formatted: Indent: Left: 0"

Formatted: Body Text, Indent: Left: 0.49", Right: 0.29", Add space between paragraphs of the same style, No bullets or numbering, Tab stops: Not at 1.5"

Formatted: Body Text, Right: 0.15"

Formatted: Body Text, Indent: Left: 0.49", Right: 0.29", Space After: 6 pt

Formatted: Indent: Left: 0.49", Right: 0.29", Space After: 6 pt

the equipment.

4. Information concerning any violation of this policy.
5. Total costs for maintenance, licensing and training, if any.
6. The results of any internal audits and if any corrective action was taken.

The above information and reporting procedures will assist in evaluating the efficacy of this policy and equipment.

D. Data Access

D – 1. OPD Data Access

OPD's RLSC system oversight as well as data retention and access, shall be managed by OPD's Information Technology Unit under the BOS, or designee.

D – 2. RLSC System Coordination

The IT Unit Coordinator is responsible for ensuring systems and processes are in place for the proper collection, accuracy and retention of live-stream camera system data. The Intel Unit Supervisor is responsible for ensuring that all use of remote utility pole installed cameras are used in accordance with all OPD policies and procedures outlined in this policy.

D – 3. Third Party Data Access

OPD may use remote cameras owned and operated by the ATF and/or other approved law enforcement partners. OPD personnel may only use camera technology from other law enforcement agencies such as the ATF with the express written permission of the Intel Unit supervisor.

RLSC system 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 RLSC data that includes:

   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The intended purpose of obtaining the information.

2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.

3. The approved request is retained on file.

Requests for RLSC data by non-law enforcement or non-prosecutorial agencies will be processed as provided in Departmental General Order M-09.1, Public

Formatted: Indent: Left: 0", Tab stops: 0.5", Left + 1", Left + 1.5", Left + 2", Left + 2.5", Left + 3", Left + 3.5", Left + 4", Left + 4.58", Left

Formatted: Font: Times New Roman, 12 pt, Bold, Not Expanded by / Condensed by

Formatted: Font: Bold, Not Expanded by / Condensed by

Formatted: List Paragraph, Right: 0", Space After: 6 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.25", Hanging: 0.5"

Formatted: Indent: Left: 0.25"

Formatted: Indent: Left: 0.25"

Formatted: Font: Not Bold

Records Access (Civil Code § 1798.90.55) and per any interagency agreements.

E. Data Retention

All RLSC data will be closely safeguarded and protected by both procedural and technological means:

1. All live-stream cameras ~~RLSCs~~ shall be housed and secured within IT Unit or ~~Intel Uni~~t lockers. All RLSC data downloaded from RLSCs shall be uploaded onto secure user and email password protected IT Unit computers and / or Intel Unit computers.

~~2.~~ For data that is captured and used as evidence, such data shall be turned in and stored as evidence. ~~Those are the protocols used PEU or IAD or RMM systems.~~

~~2.~~

3. Members approved to access RLSCs under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data related to an administrative or criminal investigation, or for training purposes.

D – 4. Training

The Training Section shall ensure that members receive department-approved training for those authorized to use or access live-stream cameras. The Intel Unit shall ensure that members authorized to view remote pole camera data are properly trained by the Intel Unit. The Training Division shall ~~the Shotspotter system and~~ shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed:

Formatted: Tab stops: 0.5", Left + 1", Left + 1.5", Left + 2", Left + 2.5", Left + 3.15", Centered

Formatted: List Paragraph, Right: 0", Space After: 6 pt, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.25"

Formatted: Indent: Left: 0", First line: 0"

Formatted: Indent: Left: 0", First line: 0", Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.75" + Indent at: 1"

Formatted: Font: (Default) Times New Roman, 12 pt, Bold

Formatted: Normal, No bullets or numbering