CITY OF OAKLAND

Privacy Advisory Commission

October 6, 2016 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:*** *Yaman Salahi,* ***District 3 Representative:*** *Brian M. Hofer,* ***District 4 Representative:*** *Lou Katz,* ***District 5 Representative:*** *Raymundo Jacquez III,* ***District 6 Representative:*** *Clint M. Johnson,* ***District 7 Representative:*** *Robert Oliver,* ***Council At-Large Representative:*** *Saied R. Karamooz,* ***Mayoral Representative:*** *Deirdre Mulligan.*

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: Review and approval of September 1 meeting minutes
3. 5:10pm: Introduction of new Commissioners
4. 5:15pm: Parking Management Strategy Report – presentation by Michael Ford
5. 5:25pm: Discuss and take possible action on a Cell-Site Simulator Policy
6. 6:40pm: Discuss and take possible action on a Surveillance Equipment Ordinance
7. 6:55pm: Open Forum
8. 7:00pm: Adjournment

This meeting location is wheelchair accessible. Do you need an ASL, Cantonese, Mandarin or Spanish interpreter or other assistance to participate? Please email jdevries@oaklandnet.com or call (510) 238-3083 or (510) 238-3254 for TDD/TTY five days in advance.

Esta reunión es accesible para sillas de ruedas. ¿Necesita un intérprete en español, cantonés o mandarín, u otra ayuda para participar? Por favor envíe un correo electrónico jdevries@oaklandnet.com o llame al (510) 238-3083 o al (510) 238-3254 Para TDD/TTY por lo menos cinco días antes de la reunión. Gracias.

會場有適合輪椅出入設施。你需要手語, 西班牙語, 粵語或國語翻譯服務嗎？請在會議前五個工作天電郵jdevries@oaklandnet.com 或致電 (510) 238-3083 或 (510) 238-3254 TDD/TTY。

CITY OF OAKLAND

Privacy Advisory Commission

September 1, 2016 5:00 PM
Oakland City Hall
Council Chambers, third floor
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Minutes

Commission Members: ***District 1 Representative:*** *Reem Suleiman,* ***District 2 Representative:*** *Yaman Salahi,* ***District 3 Representative:*** *Brian M. Hofer,* ***District 4 Representative:*** *Lou Katz,* ***District 5 Representative:*** *Raymundo Jacquez III,* ***District 6 Representative:*** *Clint M. Johnson,* ***District 7 Representative:*** *Currently Vacant,* ***Council At-Large Representative:*** *Saied R. Karamooz,* ***Mayoral Representative:*** *Currently Vacant.*

Commission Website: http://www2.oaklandnet.com/OAK057463

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

Members Present: *Hofer, Katz, Jacquez, Johnson, Karamooz, Suleiman, Salahi.*

Members Absent: *None.*

2. 5:05pm: Review and approval of August 11 meeting minutes

The August 11, 2016 minutes were approved unanimously with one edit to a typo noted.

3. 5:10pm: Discuss and take possible action on a Surveillance Equipment Ordinance and Surveillance Technology Assessment Questionnaire.

Chairperson Hofer provided an overview of the purpose of the ordinance, noting the intent is to have a discussion at the beginning of a process to acquire and use surveillance technology instead of after

technology has been acquired. The ordinance is a way to outline the process so there is a consistent framework that the city follows to consider such technology. He outlined the purpose of each section from the information gathering stage to the findings required by the City Council to acquire equipment, to the follow-up impact reporting and items such as non-disclosure agreements and potential penalties for violation.

Member Johnson noted some proposed changes; specifically he would remove Paragraph 2 in the introduction as it seems negative and doesn't serve a real purpose. He also would take out the reference to wiretaps in section 3, and in paragraph 5 he would take out "significant weight" and replace it with "fair and meaningful consideration."

Member Katz asked if section 2 could provide better clarity regarding gifts and donations and in section 4H he noted concerns about third party data management. He also suggested added language to add to section 5D to include "entities, organizations, and corporations." In Section 5F he would add language explicitly referencing deleting data from "back-ups" to see that all data that should be deleted is actually deleted.

Member Salahi raised a concern about when the annual reports are presented; he wants to avoid a bottleneck of reports at one time of year and suggests if they are spread out it will make the commission's work more manageable. Regarding third party access he believes the ordinance requires the City to be transparent about whether a third party is involved in any data management. He raised concern about removing paragraph 2 because he believes it is important to articulate why the City has a privacy Commission. In Section 8, paragraph 3, he suggests that the ordinance change and to or so that if a private party seeks to enforce the ordinance they will be able to recover fees in either situation.

Member Suleiman asked if there were any administrative restrictions preventing the Commission from staggering the annual reports referring to member Salahi's concern. Joe DeVries noted that the Commission could postpone reports but if that postponement stopped an agency from using the equipment when that agency had submitted the report on time, this would be problematic. He went on to note the 180 day deadline for agencies to submit reports on existing technology could be problematic for similar reasons. The City would not want to violate the ordinance but if it cannot produce the requested inventory of reports and impact assessments within 180 days, it could not afford to simply stop using equipment that had been in use for long periods of time already.

Chairperson Hofer noted the 180 days is a suggestion and since this is new, the intent is to move to compliance, not to try to catch the City in a violation. He suggested language can be added allowing for an exception or an extension.

On that subject Member Katz recommended wording that prevents the Commission from acting by failing to act—in other words, the Commission cannot simply refuse to hear a report to prevent an item from being used.

Joe DeVries commented that the timelines are critical to have the Police Department (and other departments) explain the typical process for applying for grants to make sure timeline are not created that will eliminate the ability to apply at all. He cited some former federal grants he was involved in where the application period was faster than the timelines currently written in the draft.

Deputy Chief Lois addressed the Commission on this same item—noting that he would speak with his fiscal and policy departments to see what type of timeline would be workable and get to the objectives of the Commission.

Ahsan Baig from the IT Department noted that there are many different types of applications from various agencies so it's hard to provide a standard type. However, alerting the Commission when an application is being prepared is possible.

Member Karamooz noted he thinks it would be great to get notice to the Commission as an application is being prepared to prevent the agency from doing too much work on an application that will raise large concerns much further along in the process. Member Katz asked if there are public records of grant applications being drafted. DC Lois committed to check in with staff and report back on this at the next meeting.

Chairperson Hofer asked about section 5 and the process for addressing previously existing technology. It was noted that after the effort to address previous technology is completed, the workload will be much lower. However, the Commission needs to know how many different items exist currently that need to be assessed. This section really needs to be vetted to determine that initial impact.

Chairperson Hofer asked staff to also look at the impact report and allowable use policy sections and provide as much feedback as possible to make sure the ordinance is workable. Ahsan Baig noted he would be looking a lot more closely at the draft and would be able to provide more input at the next meeting.

Chairperson Hofer recapped that OPD and IT would survey current technologies to give a better idea of how many currently exist that will need to be assessed and the City Administrator could make a recommendation on the time deadline based on this information.

Chairperson Hofer noted he would incorporate the concerns raised in the next draft that he brings back.

Public Speakers were called:

Brian Geiser noted that there are two items listed under item 3 and when speakers are called before the second part is considered it potentially prevents them from commenting on it. He also noted that when the Commission drafts ordinances, it would help the public to see the changes made from meeting to meeting to be able to track the progress. He also suggested that the Commission's reports come to the City Council twice a year to keep it fresh in their minds and that the timing be such that it can promote conversation during the budget discussions so that it resources need to be allocated it will happen.

There was some brief conversation about the Surveillance Technology Questionnaire which Member Karamooz and Hofer had edited portions of since the last meeting.

Member Katz raised concerns about future alterations to technologies (especially by third parties) that happen after the public review. He noted that software upgrades occur all the time and if they modify a technology's capabilities, they need to be reviewed.

Member Jaquez asked about section 1.3 of the questionnaire noting that he wants to see language about evidence of the successfulness of a particular technology as opposed to just a "success rate" which is vague. Chairperson Hofer asked about "track record" as possible language. Member Jaquez still sees that as vague—he wants some data supporting the uses effectiveness.

4. 6:50pm: Open Forum

J.P. Masser spoke about his recalling former Mayor Quan saying that "if the Department of Homeland Security hands the City $5 million than the city is going to use it" so he wants to be sure the mere submission of an application is not justification supporting a particular use.

5. 7:00pm: Adjournment

CITY OF OAKLAND

AGENDA REPORT

TO:	Sabrina B. Landreth City Administrator	**FROM:**	David E. Downing Assistant Chief of Police
SUBJECT:	Cell-Site Simulator Technology	**DATE:**	September 26, 2016

City Administrator Approval | Date

RECOMMENDATION

Staff Recommends That The City Council Approve A Resolution Authorizing The City Administrator Or Designee To Enter Into A Memorandum Of Understanding (MOU) With The Alameda County District Attorney's Office (ACDA) For The Purpose Of Allowing Members Of The Oakland Police Department (OPD) To Use Cellular Site Simulator (CSS) Technology, For Five Years From The Effective Date Of The MOU At No Cost To OPD.

EXECUTIVE SUMMARY

Approval of this MOU will allow OPD to enter into a no-cost MOU with ACDA to use CSS technology to assist missing persons, at-risk individuals, and victims of ~~natural disasters~~mass casualty incidents; investigations involving danger to the life or physical safety of individuals; as well as in the apprehension of fugitives.

BACKGROUND AND LEGISLATIVE HISTORY

California Government Code § 53166(b) was enacted in October 2015 and regulates the use of CSS technology by law enforcement agencies. Among other provisions, the law states that law enforcement agencies using CSS technology must maintain reasonable security procedures and practices. The law also requires that law enforcement agencies using CSS technology "[i]mplement a usage and privacy policy to ensure that the collection, use, maintenance, sharing, and dissemination of information gathered through the use of cellular communications interception technology complies with all applicable law and is consistent with respect for an individual's privacy and civil liberties. This usage and privacy policy shall be...posted conspicuously on [the agency's] Web site. The usage and privacy policy shall...include...[t]he existence of [any] memorandum of understanding or other agreement with another local agency or any other party for the shared use of cellular communications interception technology or the sharing of information collected through its use, including the identity of signatory parties."[1]

[1] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=53166.&lawCode=GOV

ACDA has acquired CSS technology and is making it available to Alameda County law enforcement agencies. In order to use this technology, OPD must enter into an MOU with ACDA. A draft MOU (***Attachment A***) has been developed and requires City Council approval. A draft OPD policy (***Attachment B***) concerning use of CSS technology and making reference to the MOU with ACDA has been developed by OPD.

ANALYSIS AND POLICY ALTERNATIVES

OPD is committed to reducing crime and serving the community through fair, quality policing. OPD can more effectively save lives, reduce harm, and reduce crime through the use of CSS technology.

Authorized Purposes and Legal Authority

Per policy, OPD would be limited to using CSS technology to locate missing persons, at risk individuals, and victims of ~~natural disasters such as fire, earthquake, or flood~~mass casualty incidents. OPD would also use the technology to assist in investigations involving danger to the life or physical safety of individuals or apprehend fugitives. As provided by OPD policy, there are only two bases for use of CSS technology: with a search warrant or for an identified exigency, followed by an application for a search warrant as required by law.

What the Cell-Site Simulator Does

A CSS functions by transmitting as a cellular phone tower. Cellular devices in the area of the CSS identify the simulator as the most attractive cell tower. These cellular devices transmit signals to the CSS that identify the cellular devices. The CSS receives these signals and identifies the target device. Once the specific target device has identified the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone and reject all others. Although the CSS initially receives signals from multiple devices near the simulator while attempting to locate the target device, it does not display the unique identifying numbers of those other devices. If any unique identifier for the non-targeted device exists in the simulator, it will be purged at the end of the operation, as per policy.

(a) When used for search and rescue, the CSS will obtain signaling information from all devices in the target vicinity to locate persons in need of assistance or to further recovery efforts. Any such information will be used only for these limited purposes. All such information received will be purged as soon as the person or persons in need of assistance have been located, and in any event no less than once every 10 days~~at the end of the operation~~, as per policy.

The only information obtained by the CSS are the azimuth[2], signal strength, and device identifier.

[2] An angular measurement in a spherical coordinate system.

What the Cell-Site Simulator Does Not Do

The CSS owned by ACDA and available to OPD through MOU is incapable of capturing emails, texts, contact lists, images or any other data. The CSS is also incapable of collecting subscriber account information such as an account holder's name, address, or telephone number. Per policy, any data that is acquired by the cell-site simulator device will be deleted at the end of any 24-hour period of use unless needed for a search and rescue operation. Any data acquired during a search and rescue operation will be deleted at the end of the operation, as per policy.

Oversight by OPD

The OPD cell-site simulator policy and the resolution that accompanies this report require that each use of cell-site simulator technology by OPD must be approved by the Chief of Police or Assistant Chief of Police. Any emergency use must be approved by a Lieutenant of Police or higher-ranking member, as per policy and the accompanying resolution. The Chief of Police, Privacy Advisory Commission, and the Public Safety Committee will be provided with an annual report that includes information on each use of cell-site simulator technology.

PUBLIC OUTREACH / INTEREST

OPD staff presented this report to the Privacy Advisory Commission on August 11, 2016. This presentation followed a meeting and correspondence with Brian Hofer, Chair of the Privacy Commission. The policy will be placed on the OPD website upon City Council approval of the accompanying resolution.

COORDINATION

This report and legislation have been reviewed by the Office of the City Attorney.

FISCAL IMPACT

There is no expected fiscal impact for this MOU. OPD staff time will be required to use the CSS. Any such staff time will rely on existing funding in the General Purpose Fund.

SUSTAINABLE OPPORTUNITIES

Economic: There are no economic opportunities associated with this report.

Environmental: There are no environmental opportunities associated with this report.

Social Equity: All residents benefit from greater public safety. Inter-agency partnerships allow OPD to enhance its investigative capacity. Successful investigations and more prosecutions of criminal activity will likely occur from the implementation of this MOU.

ACTION REQUESTED OF THE PUBLIC SAFETY COMMITTEE

Staff Recommends That The City Council Approve A Resolution Authorizing The City Administrator Or Designee To Enter Into A Memorandum Of Understanding (MOU) With The Alameda County District Attorney's Office (ACDA) For The Purpose Of Allowing Members Of The Oakland Police Department (OPD) To Use Cellular Site Simulator (CSS) Technology, For Five Years From The Effective Date Of The MOU At No Cost To OPD.

For questions regarding this report, please contact Bruce Stoffmacher, Legislation Manager, OPD Research and Planning, at (510) 238-6976.

Respectfully submitted,

David E. Downing
Assistant Chief of Police
Oakland Police Department

Prepared by:
Bruce Stoffmacher, Legislation Manager
OPD, Research and Planning, OCOP

Attachments (2)
A: Draft MOU with ACDA Concerning Cell-Site Simulator Technology
B: Draft OPD Policy Concerning Cell-Site Simulator Technology

Memorandum of Understanding
Between
The Alameda County District Attorney's Office
and
The Oakland Police Department

I. PARTIES – PARTICIPATING AGENCIES

This agreement, referred to herein as a "Memorandum of Understanding" (MOU) is entered into by and between the law enforcement agencies collectively referred to herein as "Participating Agencies", specifically the:

A. Alameda County District Attorney's Office (ACDA)
B. Oakland Police Department (OPD)

A "Participating Agency" is an allied state or local law enforcement agency that has made a commitment of resources for an agreed upon period of time. This commitment is on a case by case basis to access and deploy the specific equipment and technology referred to herein as the "CSS Program."

PARTICIPATING AGENCIES HEREBY AGREE AS FOLLOWS:

II. PURPOSE/MISSION

OPD desires access to Cellular-Site Simulator (CSS) technology and equipment possessed and controlled by ACDA, to enhance investigative capabilities. This includes the ability to quickly and safely apprehend fugitives, locate missing and at risk individuals, provide search and rescue support in natural disasters and emergencies, and locate persons involved in serious crimes that put the public at risk.

This MOU is sets forth of the terms and conditions of access to the CSS Program. This MOU outlines responsibilities of participating agencies as they relate to the requirements for pre-deployment, deployment, use and post-use of the CSS Program technology and equipment. As with any law enforcement capability, ACDA and OPD must use the CSS Program in a manner consistent with the requirements and protections of the United States Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register Statute. Information resulting from the use of a cell-site simulator must be handled consistent with applicable statutes, regulations, and policies that guide law enforcement in the collection, retention, and disclosure of data.

The mission of the CSS Program is to enhance public safety by acquiring real time intelligence to:

- Increase opportunities to protect the public, enhance officer safety, and reduce deadly force encounters.
- Apprehend fugitives.
- Locate missing or at risk individuals.
- Locate victims of natural disasters.

III. EFFECTIVE DATE/DURATION/TERMINATION

A. This MOU shall become effective upon execution by all their respective representatives.

B. The term of this MOU is five years from the effective date.

C. The participating agencies will review the mission objectives and the need for continued operation under this MOU every 12 months.

D. Either agency may withdraw from this agreement by written notice. Written notice of intent to withdraw must be provided to the other participating agencies within 30 days prior to the date of the intended withdrawal.

E. Any amendment or extension shall be agreed upon by both parties.

IV. PROGRAM OVERSIGHT, MANAGEMENT, AND SUPERVISION

A. PROGRAM OVERSIGHT COMMITTEE

1. The Program Oversight Committee (Committee) shall be comprised of the Chief's designee from each participating agency.

2. The Committee shall meet annually to review and assess:

    a. Program policies and procedures
    b. Pre-deployment requirements
    c. Operational guidelines
    d. Reports of deployment
    e. Policy compliance
    f. Equipment condition
    g. MOU terms and provisions

3. The Committee shall prepare a report to summarize its review and assessment and provide the report to each participating agency's Chief within ten days of completing the review and assessment.

B. PROGRAM MANAGEMENT

1. ACDA Responsibilities:

a. Assess and approve or deny CSS Program deployment requests

b. Management and daily operation of the CSS Program

c. Developing and preparing CSS Program policies and operating procedures

d. Media releases regarding the CSS Program and its use

e. CSS Program equipment maintenance and storage in a secured facility

f. CSS Program equipment operating costs

2. Participating Agency Responsibilities

The following provisions will guide the participating agencies regarding resources, deployment, policy, training, and supervision.

a. Each participating agency shall commit personnel to staff the CSS Program. ACDA will assign staff to each participating agency CSS Program deployment to assist with and monitor use of the equipment, data collection, and policy compliance.

b. Each participating agency will assign supervisors and equipment operators (Operators) to the CSS Program. The personnel initially assigned to the CSS Program will be listed on Attachment A to this MOU. Additions, deletions, and temporary reassignments of personnel will be at the discretion of the respective participating agencies, with notice to the other participating agencies.

c. Each participating agency will provide for the salary and employment benefits, including overtime, of their personnel assigned to the CSS Program. Each participating agency will retain control of its personnel's work hours, including the approval of overtime.

d. Each participating agency shall designate qualified personnel (Operators) to complete training to operate the equipment and appropriately manage data obtained through its use. Only properly trained peace officers may

operate the CSS Program equipment. Training is completed at the participating agency's expense.

e. CSS Program Operators must meet the following minimum qualifications:

1. Must be Peace Officers (830.1 PC)
2. Must complete required training
3. Must be familiar with the ACDA policy "Use of a Cell-Site Simulator"
4. If operating the CSS vehicle, must have a valid California Driver's License

f. CSS Program Coordinators

Each participating agency agrees to designate a Program Coordinator (Coordinator) to the CSS Program. These Coordinators are responsible for insuring compliance with this MOU and all related policies affecting CSS Program deployment and operations. The personnel assigned as Coordinators will be listed on Attachment B to this MOU. Additions, deletions, and temporary reassignments of personnel will be at the discretion of the respective participating agencies, with notice to the other participating agencies.

g. Operational Dispute Mediation

Operational disputes will normally be mutually addressed and resolved by the on-scene designated CSS Program supervisors. Any problems not resolved at this level will be referred to the CSS Program Coordinators identified in Attachment B of this MOU. However, the ACDA Chief of Inspectors or his/her designee is vested with the authority to resolve any dispute and to reverse decisions made at any level. Decisions by the ACDA Chief of Inspectors are final.

h. Identifying Cases for Deployment

The ACDA Chief of Inspectors or his/her designee shall assess and approve or deny each request for deployment based on the criteria set forth below.

The participating agencies agree to limit requests to use CSS Program resources to the following:

1. **Pursuant to a search warrant**[1]:

    a. Investigations involving danger to the life or physical safety of an individual.

    b. Apprehension of a fugitive.

2. **Emergency**:

    a. The CSS program may be used, absent a search warrant, if a participating agency, in good faith, believes that *an emergency* involving danger of death or serious physical injury to any person exists.

    b. Search and rescue operations

    c. Missing or at risk person operations

    d. Warrantless CSS Program deployments must be approved per the provisions of this MOU.

C. PROGRAM SUPERVISION

1. Operations

    The Operator Supervisor is responsible for initiating, assigning, directing, monitoring, supervising, concluding and reporting CSS Program deployments for their respective agency.

2. Reporting (deployment)

    The Operator Supervisor shall complete, consistent with applicable procedures, the required Incident Report to document the participating agency's use of the CSS Program equipment and will forward the report to the ACDA Chief of Inspectors within five days of concluding a CSS Program deployment.

3. Reporting (equipment)

    The Operator Supervisor shall complete, consistent with applicable procedures, the required Incident Report to document any equipment failure, equipment damage or operational concern(s) related to

[1] Any valid search warrant, including telephonic search warrants, satisfy this requirement.

equipment and will forward the report to the ACDA Chief of Inspectors as soon as is practical.

4. Complaints (personnel)

   Each participating agency shall be responsible for receiving, investigating and adjudicating any personnel complaint(s) regarding their employee(s) arising out of the use of the CSS Program equipment or use of data obtained by the equipment.

5. General Guidelines

   While all personnel assigned to the CSS Program will give primary consideration to the regulations and guidelines imposed by their own agency, they shall not violate policies and procedures imposed by the ACDA regarding the CSS Program. ACDA policies and procedures are controlling when participating agencies, authorized by this MOU, are assigned to a CSS Program deployment operation.

   Each participating agency member assigned to the CSS Program will be provided with copies of the relevant ACDA policies and procedures. Participating agencies' policies may be more restrictive than ACDA policies in their decisions to request deployments of the CSS Program equipment. In those instances where participating agencies' policies are more restrictive that ACDA, then the participating agencies' policies are controlling.

V. OUTSIDE AGENCY REQUESTS

Outside agency requests for use of the CSS Program may be directed to any of the participating agencies. The participating agency shall forward the request only if the outside agency request meets the criteria described herein and the requesting agency's search warrant includes the Pen-Register and request for the use of the Cell-Site Simulator. It is the responsibility of the participating agency to review the search warrant and ensure that it is accurate and that there is probable cause to justify deployment. Participating agencies shall forward policy compliant requests to the ACDA Chief of Inspectors or his or her designee. If the request is (a) warrantless, ~~and~~ (b) an emergency, and (c) meets the criteria described in Part 4.B.2.h.2. of this MOU, ~~if possible,~~ the request ~~shall~~ may be granted.

VI. REPORTING

ACDA will prepare and provide an Annual Report of CSS Program deployment activity to the Alameda County Board of Supervisors no later than February 15th of each year. The report will summarize the preceding calendar year's program activities.

VII. MEDIA RELATIONS

1. CSS Program (general inquiries)

   Media relations specific to the CSS Program, program equipment, program technology and program policies and procedures will be handled by the ACDA Public Information Officer.

   Participating agencies will refer all press and media requests and inquiries regarding the CSS Program, program equipment, program technology and program policies and procedures to the ACDA Public Information Officer to the extent permissible by law.

2. CSS Program Deployments

   Participating agencies will not give statements or release information to the media regarding any CSS Program deployment without the concurrence, where appropriate, of the prosecuting attorney and the ACDA Public Information Officer to the extent permissible by law.

VIII. PROGRAM AUDIT

The operations under this MOU are subject to audit by the ACDA. OPD agrees to permit such audits and to maintain records relating to the terms, provisions and compliance of this agreement for the term of this MOU and, if an audit is being conducted, until such time as the audit is officially completed, whichever is greater. These audits may include review of any and all records, documents, and reports relating to this MOU, as well as the interview of any and all personnel involved in relevant CSS Program deployment operations. Examples of records are:

- Program Operator Training Record
- Search Warrant and Affidavit
- Agency policies and procedures

IX. LIABILITY

Notwithstanding any other agreements, the City of Oakland agrees to hold harmless and indemnify Alameda County and/or ACDA against any legal liability with respect to bodily injury, death, and property damage arising out of the City's use of CSS equipment belonging to Alameda County and/or ACDA pursuant to this agreement except for such losses or damages which were caused by the sole negligence or willful misconduct of ACDA.

Further, Alameda County and/or ACDA agrees to hold harmless and indemnify the City of Oakland against any legal liability with respect to bodily injury, death, and

property damage arising out of the ACDA's use CSS equipment belonging to the AC and/or ACDA pursuant to this agreement except for such losses or damages which were caused by the sole negligence or willful misconduct of the City of Oakland.

X. NOTICES

Unless otherwise indicated elsewhere in this agreement, all written communications sent by the parties may be by U.S. mail, email or by facsimile, and shall be addressed as follows:

To: **Alameda County District Attorney's Office**
Lieutenant Daniel Lee
Alameda County District Attorney's Office
1225 Fallon Street
Oakland, California
Phone: (510) 208-9879
Fax: (510) 271-5157
Email: daniel.lee@acgov.org

To: **Oakland Police Department**
Deputy Chief Darren Allison
Oakland Police Department
455 7th Street
Oakland, California 94607
Phone: (510) 238-3958
Fax: (510) 637-0166
Email: dallison@oaklandnet.com

XI. REVISIONS

The terms of this MOU may be amended, modified, or revised in writing. Such amendment, modification, or revision will become effective upon the signatures of authorized representatives of all of the participating agencies.

IX. SIGNATORIES

By: _____ Date: _____
Name: Nancy E. O'Malley
Title: District Attorney
Agency: Alameda County District Attorney's Office

By: _____ Date: _____
Name: Robert Chenault
Title: Chief of Inspectors
Agency: Alameda County District Attorney's Office

By: _____ Date: _____
Name: David E. Downing
Title: Assistant Chief of Police
Agency: Oakland Police Department

Policy
XXX

Oakland Police Department
Policy Manual

Cellular Site Simulator Usage and Privacy

XXX.1 PURPOSE AND SCOPE

The purpose of this policy is to set guidelines and requirements pertaining to cellular-site simulator technology usage and privacy.

XXX.2 POLICY

It is the policy of the Oakland Police Department to respect the privacy rights of individuals and to follow the Constitution and all applicable laws.

XXX.3 BASIS FOR POLICY

Government Code § 53166(b) requires all law enforcement organizations that use cellular communications interception technology, including cellular site simulator technology, to:

(a) Maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect information gathered through the use of cellular communications interception technology from unauthorized access, destruction, use, modification, or disclosure.

(b) Implement a usage and privacy policy to ensure that the collection, use, maintenance, sharing, and dissemination of information gathered through the use of cellular communications interception technology complies with all applicable law and is consistent with respect for an individual's privacy and civil liberties. This usage and privacy policy shall be available in writing to the public, and, if the local agency has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site. The usage and privacy policy shall, at a minimum, include all of the following:

1. The authorized purposes for using cellular communications interception technology and for collecting information using that technology.
2. A description of the job title or other designation of the employees who are authorized to use, or access information collected through the use of, cellular communications interception technology. The policy shall identify the training requirements necessary for those authorized employees.
3. A description of how the local agency will monitor its own use of cellular communications interception technology to ensure the accuracy of the information collected and compliance with all applicable laws, including laws providing for process and time period system audits.
4. The existence of a memorandum of understanding or other agreement with another local agency or any other party for the shared use of cellular communications interception technology or the sharing of information collected through its use, including the identity of signatory parties.
5. The purpose of, process for, and restrictions on, the sharing of information gathered

through the use of cellular communications interception technology with other local agencies and persons.

6. The length of time information gathered through the use of cellular communications interception technology will be retained, and the process the local agency will utilize to determine if and when to destroy retained information.

Members shall only use approved devices and usage shall be in compliance with department security procedures, the department's usage and privacy procedures and all applicable laws.

XXX.4 HOW THE TECHNOLOGY WORKS

Cellular site simulator technology relies on use of cellular site simulators. Cellular site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the simulator identify it as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would a networked tower.

A cellular site simulator receives signals and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider to distinguish between incoming signals until the targeted device is located. Once the cellular site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone, rejecting all others. Although the cellular site simulator initially receives signals from multiple devices in the vicinity of the simulator while attempting to locate the target device, it does not display the unique identifying numbers of those other devices for the operator. To the extent that any unique identifier for the non-targeted device might exist in the simulator itself, it will be purged at the conclusion of operations in accordance with this policy.

When used in a ~~natural disaster~~mass casualty or other emergency situation, or to aid search and rescue efforts, the cellular site simulator will obtain signaling information from all devices in the simulator's target vicinity for the limited purpose of locating persons in need of assistance or to further recovery efforts. Any information received from the cellular devices during this time will only be used for these limited purposes and all such information received will be purged at the conclusion of the effort in accordance with this policy.

XXX.4.1 INFORMATION OBTAINED

By transmitting as a cell tower, cellular site simulators acquire identifying information from cellular devices. As employed by the Oakland Police Department, this information is limited. Cellular site simulators provide only the relative signal strength and general direction of a subject cellular telephone. They do not function as a GPS locator, as they will not obtain or download any location information from the device or its applications. Cellular site simulators used by the Oakland Police Department ~~will can not~~cannot be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). ~~This limitation will be made an express part of any search warrant sought by the Oakland Police Department.~~

Cellular Site Simulator Privacy and Usage

The cellular site simulator ~~will can not~~cannot capture emails, texts, contact lists, images or any other data contained on the phone. In addition, the cellular site simulators do not collect subscriber account information (for example, an account holder's name, address, or telephone number). ~~The cellular site simulator sought to be used by the Oakland Police Department does not have the capacity to intercept or capture communications, emails, texts, contact lists, images or other data contained on the device.~~

XXX.5 AUTHORIZED PURPOSES

The authorized purposes for using cellular communications interception technology and for collecting information using that technology to:

(a) Locate missing persons
(b) Locate at-risk individuals
(c) Locate victims of ~~natural disasters~~mass casualty incidents ~~(fire, earthquake, flood)~~
(d) Assist in investigations involving danger to the life or physical safety of an individual
(e) Apprehend fugitives

XXX.5.1_LEGAL AUTHORITY

Cellular site simulator technology will be used by the Oakland Police Department only with a search warrant or for an identified exigency, followed by an application for a search warrant as required by law.

When making any application to a court, members of the Oakland Police Department must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought. Oakland Police Department personnel must consult with prosecutors when using a cell-site simulator and applications for the use of a cell- site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.

(a) Regardless of the legal authority relied upon, at the time of making an application for use of a cell-site simulator, the application or supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine the physical location of the target cellular device.

(b) An application or supporting affidavit should inform the court that the target cellular device (e.g., cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider. The application may also note, if accurate, that any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.

(c) An application for the use of a cell-site simulator should inform the court about how law enforcement intends to address deletion of data not associated with the target phone. The application should also indicate that law enforcement will make no affirmative use of any non-target data, except to identify and distinguish the target device from other devices.

If cellular site technology is used based on an exigency, then the above requirements will be met when applying for the search warrant within 48 hours after use. An exigency is defined as an imminent threat of death or bodily injury.

XXX.6 JOB TITLES, DESIGNATIONS, AND TRAINING REQUIREMENTS

Personnel authorized to use or access information collected through the use of cellular communications interception technology shall be specifically trained in such technology and authorized by the Chief of Police or designee. Such personnel shall be limited to designated sergeants and officers unless otherwise authorized.

Training requirements for the above employees include completion of training by the manufacturer of the cellular communications interception technology or appropriate subject matter experts as designated by the Oakland Police Department. Such training shall include Federal and state law; applicable policy and memoranda of understanding; and functionality of equipment. Training updates are required annually.

XXX.7 AGENCY MONITORING AND CONTROLS

The Oakland Police Department will monitor its use of cellular site simulator technology 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 Chief of Police shall designate a Cellular Site Simulator Program Supervisor who shall ensure such audits are conducted in accordance with law and policy.

XXX.7.1 DEPLOYMENT LOG

Prior to deployment of the technology, use of a cellular site simulator by the Oakland Police Department must be approved by the Chief of Police or the Assistant Chief of Police. Any emergency use of a cellular site simulator must be approved by a Lieutenant of Police or above. Each use of the cellular site simulator device requires completion of a log by the user. The log shall include the following information at a minimum:

(a) The name and other applicable information of each user.
(b) The reason for each use.
(c) The results of each use including the accuracy of the information obtained.

XXX.7.2 ANNUAL REPORT

The Cellular Site Simulator Program Coordinator shall provide the Chief of Police, the Privacy Advisory Commission, and Public Safety Committee with an annual report that contains all of the above information. The report shall also contain the following for the previous 12-month period:

(a) The number of times cellular site simulator technology was requested.
(b) The number of times cellular site simulator technology was used.
(c) The number of times that agencies other than the Oakland Police Department received information from use of the equipment by the Oakland Police Department.
(d) Information concerning any violation of this policy.
(e) Total costs for maintenance, licensing and training, if any.

(f) The results of any internal audits and if any corrective action was taken, subject to laws governing confidentiality of employment actions and personnel rules.
(g) How many times the equipment was deployed to:
1. Make an arrest or attempt to make an arrest.
2. Locate an at-risk person.
3. Aid in search and rescue efforts.
(h) If cellular site simulator technology was used in relation to a crime, the type of crime.
(i) The effectiveness of the technology in assisting in investigations.

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

XXX.8 MEMORANDUM OF UNDERSTANDING
The Oakland Police Department has a memorandum of understanding with the Alameda County District Attorney's Office for the shared use of cellular site simulator technology and the sharing of information collected through its use. The signatory parties are the County of Alameda and the City of Oakland.

XXX.9 SHARING OF INFORMATION
The Oakland Police Department will share information gathered through the use of cellular site simulator technology with other law enforcement agencies with 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 investigation.

Information will be shared only with agencies in accordance with a lawful purpose and limited to a court order, search warrant, or identified exigency. The Oakland Police Department will not share information outside of the legal parameters necessary for the lawful purpose. All requests for information shall be reviewed by the Cellular Site Simulator Program Coordinator or other individual as designated by the Chief of Police. Information will be shared only upon approval of the Cellular Site Simulator Program Coordinator or other individual as designated by the Chief of Police.

The agency with which information is shared ("recipient agency") shall be designated as the custodian of such information. The recipient agency shall be responsible for observance of all conditions of the use of information including the prevention of unauthorized use, retention of information, and destruction of information.

Every law enforcement agency and officer requesting use of the cell- site simulator, shall be provided with a copy of this Policy and specialized training in the use of this technology. Such agencies shall also provide copies of this Policy and training, as appropriate, to all relevant employees who may be involved in the use of this technology.

XXX.10 RETENTION AND DISPOSAL OF INFORMATION
The Oakland Police Department shall destroy all information intercepted by the cellular site simulator equipment as soon as the objective of the information request is accomplished and shall record this destruction in accordance with the following:

Cellular Site Simulator Privacy and Usage

(a) When the cellular site simulator equipment is used to locate a known cellular device, all data shall be deleted upon locating the cellular device and no fewer than once daily for a known cellular device.

(b) When the cellular site simulator equipment is used in a search and rescue operation, all data must be deleted ~~immediately upon completion of the operation.~~as soon as the person or persons in need of assistance have been located, and in any event no less than once every 10 days.

(c) Prior to deploying the cellular site simulator equipment for a subsequent operation, ensure the equipment has been cleared of any previous operational data.

(d) No data derived recorded by cellular site simulator equipment will be stored on any server, device, cloud-based storage system, or in any capacity.

Approved as to Form and Legality

City Attorney

OAKLAND CITY COUNCIL

RESOLUTION NO._____C.M.S.

Introduced by Councilmember _____

RESOLUTION AUTHORIZING THE CITY ADMINISTRATOR OR DESIGNEE TO ENTER INTO A MEMORANDUM OF UNDERSTANDING (MOU) WITH THE ALAMEDA COUNTY DISTRICT ATTORNEY'S OFFICE (ACDA) FOR THE PURPOSE OF ALLOWING MEMBERS OF THE OAKLAND POLICE DEPARTMENT (OPD) TO USE CELLULAR SITE SIMULATOR TECHNOLOGY, FOR FIVE YEARS FROM THE EFFECTIVE DATE OF THE MOU AT NO COST TO OPD

WHEREAS, the OPD is committed to reducing crime and serving the community through fair, quality policing; and

WHEREAS, cellular site simulator technology is available at no cost to OPD from ACDA; and

WHEREAS, OPD can more effectively investigate such crimes when provided with additional resources including the use of advanced technology; and

WHEREAS, cellular site simulator technology may only be used to locate missing persons, at-risk individuals, and victims of ~~natural disasters~~mass casualty incidents; investigations involving danger to the life or physical safety of individuals; and to apprehend fugitives; and

WHEREAS, cellular site simulator technology will be used only in a manner consistent with the Fourth Amendment to the United States Constitution and applicable statutory authorities;

WHEREAS, cellular site simulator technology will be used only pursuant to a search warrant, or identified exigency pursuant to a search warrant or identified exigency followed by an application for a search warrant as required by law; and

WHEREAS, cellular site simulator technology is incapable of being used to capture emails, texts, contact lists, images or any other data; and

WHEREAS, cellular site simulator technology is incapable of ~~being used to~~ collecting subscriber account information such as an account holder's name, address, or telephone number; and

WHEREAS, the cellular site simulator sought for use by OPD does not have the capacity to intercept or capture communications, emails, texts, contact lists, images or other data contained on a device; and

WHEREAS, only designated OPD personnel may use cellular site simulator technology; and

WHEREAS, each use of cellular site simulator technology by OPD must be approved by the Chief of Police or Assistant Chief of Police and any emergency use must be approved by a Lieutenant of Police or higher-ranking member; and

WHEREAS, the Chief of Police, the Privacy Advisory Commission, and the Public Safety Committee will be provided with an annual report that includes information on each use of cellular site simulator technology; and

WHEREAS, all data contained by the cellular site simulator device shall be deleted at the end of any 24-hour period of use unless needed for a search and rescue operation; now, therefore, be it

RESOLVED: That the City Council authorizes the City Administrator or designee to enter into a MOU with ACDA for the purpose of using cellular site simulator technology owned by ACDA at no cost to OPD for a period of five years; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to use cellular site simulator technology in a manner consistent with the Fourth Amendment to the United States Constitution and applicable statutory authorities; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to use cellular site simulator technology only pursuant to a search warrant or identified exigency followed by an application for a search warrant as required by law or following a mass casualty incident; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to use cellular site simulator technology incapable of capturing emails, texts, contact lists, images or any other data; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to use cellular site simulator technology incapable of collecting subscriber account information such as an account holder's name, address, or telephone number; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to use cellular site simulator technology that does not have the capacity to intercept or capture communications, emails, texts, contact lists, images or other data contained on a device; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to limit use of cellular site simulator technology to designated OPD personnel; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to require approval by the Chief of Police or Assistant Chief of Police for each use and approval by a Lieutenant of Police or higher-ranking member for each emergency use; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to require an annual report to the Chief of Police, the Privacy Advisory Commission, and the Public Safety Committee concerning each use of cellular site simulator technology; and be it

FURTHER RESOLVED: That the City Council authorizes the City Administrator or designee to require that all data contained by the cellular site simulator device be deleted at the end of any 24-hour period of use unless needed for a search and rescue operation; and be it

FURTHER RESOLVED: That the City Administrator, or designee, is authorized to conduct all negotiations, applications, agreements, and related actions which may be necessary to administer the aforementioned program.

IN COUNCIL, OAKLAND, CALIFORNIA, _____

PASSED BY THE FOLLOWING VOTE:

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

NOES -

ABSENT -

ABSTENTION -

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

The City Council finds it is essential to have an informed public debate as early as possible about decisions related to surveillance technology.

The City Council finds that, while 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.

The City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also 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.

The City Council finds that no decisions relating to 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.

The City Council finds that any and all decisions regarding if and how surveillance technologies should be funded, acquired, or used should include meaningful public input and that public opinion should be given significant weight.

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 surveillance technology is deployed.

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, BE IT ORDAINED that the City Council of Oakland adopts the following:

Section 1. Title

This ordinance shall be known as the Surveillance & Community Safety Ordinance.

Section 2. City Council Approval Requirement

1) A City entity must obtain City Council approval, subsequent to a mandatory, properly-noticed, germane, public hearing prior to any of the following:
    a) Seeking funds for surveillance technology, including but not limited to applying for a grant or soliciting or accepting state or federal funds or in-kind or other donations;
    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 for a purpose, in a manner or in a location not previously approved by the City Council; or
    d) Soliciting proposals for or entering into an agreement with a non-City entity to acquire, share or otherwise use surveillance technology or the information it provides.
2) A City entity must obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsection (1)(b)-(d).

Section 3. Information Required

1) The City entity seeking approval under Section 2 shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy at least forty-five (45) days prior to the public hearing. A Surveillance Use Policy shall be considered a draft proposal until such time as it is approved pursuant to a vote of the City Council.
    a) Prior to seeking City Council approval under Section 2, the City entity shall submit the Surveillance Impact Report and proposed Surveillance Use Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting.
    b) The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy.
2) After receiving the recommendation of the Privacy Advisory Commission, the City Council shall publicly release in print and online the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least thirty (30) days prior to the public hearing.
3) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 2(1).

Section 4. Determination by City Council that Benefits Outweigh Costs and Concerns

The City Council shall only approve any action described in Section 2, subsection (1) or Section 5 of this ordinance 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.

Section 5. Compliance for Existing Surveillance Technology

Each City entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a Surveillance Impact Report and a proposed Surveillance Use Policy in compliance with Section 3 (1) (a-b), and no later than one hundred eighty (180) days following the effective date of this ordinance for review and approval by the City Council pursuant to Section 4. If such review and approval has not occurred within sixty (60) days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 6. Oversight Following City Council Approval

1) A City entity which obtained approval for the use of surveillance technology must submit a written Surveillance Report for each such surveillance technology to the City Council within twelve (12) months of City Council approval and annually thereafter on or before November 1.
    a) Prior to submission of the Surveillance Report to the City Council, the City entity shall submit the Surveillance Report to the Privacy Advisory Commission for its review.
    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 Surveillance Use Policy that will resolve the concerns.

2) Based upon information provided in the Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall determine whether the requirements of Section 4 are still satisfied. If the requirements of Section 4 are not satisfied, the City Council shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve any deficiencies.
3) No later than January 15 of each year, the City Council shall hold a public meeting and publicly release in print and online a report that includes, for the prior year:
    a) A summary of all requests for City Council approval pursuant to Section 2 or Section 5 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; and
    b) All Surveillance Reports submitted.

Section 7. Definitions

The following definitions apply to this Ordinance:

1) "Surveillance Report" means a written report concerning a specific surveillance technology that includes all of the following:
    a) A description of how the surveillance technology was used, including the 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 software was installed upon; 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 individual census tract as defined in the relevant year by the United States Census Bureau;
    e) A summary of community complaints or concerns about the surveillance technology, and an analysis of any discriminatory uses of the technology and effects on the public's civil rights and civil liberties, including but not limited to those guaranteed by the California and Federal Constitutions;
    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;
    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 help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
    i) Statistics and information about public records act requests, 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 entity" means any department, bureau, division, or unit of the City of Oakland.

3) "Surveillance technology" means any electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to collect, retain, 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.
    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 in Section 7(3): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (b) Parking Ticket Devices (PTDs); (c) 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; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) 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; (f) municipal agency databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology.
4) "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 and crime statistics for any location(s);
    d) **Impact:** An assessment identifying any potential impact on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups if the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm. In addition, identify specific, affirmative measures that will be implemented to safeguard the public from each such impacts;
    e) **Data Sources:** A list of all sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data;
    f) **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;
    g) **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;
    h) **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;
    i) **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,
    j) **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).

5) "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, ~~and the uses that are prohibited;~~
   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 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 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, including any training materials;
   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.

Section 8. Enforcement

1) Any violation of Resolution No. 85638 (DAC Surveillance Use Policy adopted June 2, 2015), Resolution No. 85807 (FLIR Surveillance Use Policy adopted October 6, 2015), 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 any court of competent jurisdiction to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective city agency, 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 third-party with possession, custody, or control of data subject to this Ordinance.

2) 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 any court of competent jurisdiction against any person who committed such violation 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) and punitive damages.
3) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs (1) or (2).
4) In addition, for a willful, intentional, or reckless violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding $1,000 per violation.

Section 9. Secrecy of Surveillance Technology

It shall be unlawful for the City of Oakland or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Ordinance shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Ordinance.

Section 10. Whistleblower Protections.

1) No municipal entity or anyone acting on behalf of a municipal entity 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, conditions, access to information, restrictions on due process rights, privileges of employment, 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 to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or City Council Member, 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 municipal employee or anyone else acting on behalf of a municipal entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this Ordinance.

3) Any employee or applicant who is injured by a violation of Section 10 may institute a proceeding for monetary damages and injunctive relief in any court of competent jurisdiction.

Section 11. Severability

The provisions in this Ordinance are severable. If any part of provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this

Ordinance, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 12. Construction

The provisions of this Ordinance, including the terms defined in Section 7, are to be construed broadly so as to effectuate the purposes of this Ordinance.

Section 13. Effective Date

This Ordinance shall take effect on [DATE].

Timeline:

I. **Section 3. Information Required - sequence**
   a. City entity seeking approval under Section 2 shall submit Impact Report/Use Policy to Privacy Commission prior to heading to Council.
   b. Privacy Commission shall act on the item within 90 days (this allows for at least 3 regular meetings, in addition to special meetings).
   c. Failure by Privacy Commission to act within 90 days enables City entity to proceed to Council.

Modifications to current draft ordinance Section 3:

Section 3. Information Required

1) The City entity seeking approval under Section 2 shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy ~~at least forty-five (45) days prior to the public hearing~~. A Surveillance Use Policy shall be considered a draft proposal until such time as it is approved pursuant to a vote of the City Council.
   a) Prior to seeking City Council approval under Section 2, the City entity shall submit the Surveillance Impact Report and proposed Surveillance Use Policy to the Privacy Advisory Commission for its review at a regularly noticed meeting.
   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 modifications to the City entity and/or City Council in writing.*
   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.
2) After receiving the recommendation of the Privacy Advisory Commission, the City Council shall publicly release in print and online the Surveillance Impact Report, proposed Surveillance Use Policy, and Privacy Advisory Commission recommendation at least *fifteen (15)* days prior to the public hearing.
3) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 2(1).

Timeline:

I. **Section 5. Existing Technology – sequence**
a. OPD shall present a survey/list of equipment/software to Privacy Commission
b. Privacy Commission shall rank list in order of potential impact to civil liberties
c. Within 90 days, OPD shall submit 4 policies to the Privacy Commission for review, beginning with the highest-ranking items as determined by Privacy Commission, and continuing thereafter every 90 days until the list is exhausted.

Modifications to current draft ordinance Section 5:

Section 5. Compliance for Existing Surveillance Technology
Each City entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a Surveillance Impact Report and a proposed Surveillance Use Policy *for each surveillance technology*, in compliance with Section 3 (1) (a-c). ~~and no later than one hundred eighty (180) days following the effective date of this ordinance for review and approval by the City Council pursuant to Section 4. If such review and approval has not occurred within sixty (60) days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.~~

a) *Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, each City entity shall present to the Privacy Advisory Commission a list of surveillance technology already possessed or used by the City entity.*
b) *The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.*
c) *Within ninety (90) days of the Privacy Advisory Commission's action in b), each City entity shall submit four (4) Surveillance Impact Reports and proposed Surveillance Use Policies to the Privacy Advisory Commission for review, beginning with the highest ranking items as determined by the Privacy Commission, and continuing thereafter every ninety (90) days until the list is exhausted.*
d) *Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission, shall enable the City entity to proceed to the City Council for approval of the item pursuant to Section 4.* If such review and approval has not occurred within *sixty (60)* days of the City Council submission date, the City entity shall cease its use of the surveillance technology until such review and approval occurs.