CITY OF OAKLAND

Privacy Advisory Commission

Special Meeting

August 11th, 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****: 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
2. 5:05pm: Review and approval of July 14 meeting minutes
3. 5:10pm: Presentation by Greg Minor on Illegal Dumping Camera pilot program. Discuss and take possible action by Commission.
4. 5:25pm: Presentation by Deputy Chief Darren Allison on Cell-Site Simulator Policy.
5. 5:35pm: Presentation by ACLU Staff Attorney Matt Cagle on Cell-Site Simulators, and Model Surveillance Equipment Ordinance.

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。

6. 5:45pm: Discuss and take possible action on Cell-Site Simulator Policy.

7. 6:15pm: Discuss draft Surveillance Equipment Ordinance and draft Surveillance Technology Assessment Questionnaire. No action on these items will be taken at this meeting.

8. 6:50pm: Open Forum

9. 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

July 14th, 2016 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Minutes

Commission Members: ***District 1 Representative:*** *Reem Suleiman,* ***District 2 Representative:*** *Currently Vacant,* ***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.*

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

The Privacy Advisory Commission meeting is televised and recorded by KTOP. To view the recording in its entirety, go to: http://oakland.granicus.com/MediaPlayer.php?publish_id=73891659-4de4-11e6-8170-f04da2064c47 or visit the Board website.

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

Members Present: *Suleiman, Hofer, Katz, Jacquez, Johnson, Karamooz.* ***Members absent:*** *None. Each Member took the opportunity to introduced themselves and discuss their interest in the issue. City Staff who were in attendance introduced themselves and included staff from the City Administrator's Office, Oakland Police Department, the City Attorney's Office, and the Department of Information and Technology.*

2. 5:15pm: Staff Overview of Oakland's Boards and Commissions and their Roles and Responsibilities

Joe DeVries provided a general overview of the role of Boards and Commissions in the City of Oakland. He touched on the Brown Act, the importance of a transparent public process, current vacancies, and the rules governing meetings such as having a quorum.

3. 5:25pm: Review the PAC's enabling legislation: Ordinance 13349 and the Scope of the Commission

The Commission reviewed the enabling ordinance with special attention to the purpose of the commission. Member Katz asked for clarity as to whether data sharing by the City would be covered by the commission when surveillance technology was not involved (for example, if the city released someone's home address improperly). Member Hofer noted that the ordinance has broad language that allows for recommendations to be made in such a circumstance.

4. 5:45pm: Selecting a Chair and Vice Chair (or Interim Chair and Vice Chair) of the Commission

Member Suleiman nominated Brian Hofer as the Chair of the Commission, Member Johnson seconded the motion and he was elected unanimously.

Chairperson Hofer nominated Clint Johnson as the interim Vice-Chair, Member Katz seconded the motion and he was elected unanimously.

5. 6:05pm: Discussion and (possible) adoption of Commission Bylaws

The Commission reviewed a draft set of bylaws provided by staff and adopted them unanimously. Vice Chair Johnson asked staff about the production of meeting minutes and their availability. Joe DeVries noted that the meetings are being recorded and uploaded so the entire meeting can be reviewed. He will provide "Action Minutes" that include any official action taken at the meeting.

6. 6:20pm: Setting Meeting Dates, Times, and Location.

The group decided to set the standing meeting time as the First Thursday of each month at 5pm. However, the August Meeting will be conducted on the Second Thursday of August at 5pm (August 11th).

6:30pm: Discussion of future agenda topics

Member Karamooz opened the discussion with a recommendation that the Commission develop a protocol or structure through which new topics are presented so that there is consistency moving forward. He noted that having a standardized format that includes a comprehensive checklist will help institutionalize the process so that future boards will be able to continue the work effectively.

Chairperson Hofer agreed that the most important task is developing a process that allows public input which is why he was presenting a model ordinance drafted by the ACLU that several local governments are considering. He noted that I the past the City, and particularly the City Council is asked to approve funding for a particular piece of equipment or system without a defined community input process. This can cause confusion or mistrust as the public finds out about this technology at the point the funding is being approved instead of early on in the consideration process. He cited the controversy surrounding the Domain Awareness Center (DAC) that existed until the DAC Ad Hoc Committee was created and the fact that through the public deliberative process of the DAC Committee, eventually unanimous agreement was reached about how to move forward.

He asked the Commission to look closely at the model ordinance and suggested discussion can continue through August and September. He anticipates some conflict over what constitutes surveillance technology and wants to bring in the end user (OPD staff, for example) so the commission has a real understanding of how the technology will be used. He cited the example of the Ad Hoc Committee developing a policy for the FLIR-a thermal imaging camera used on the City's helicopters. In that instance, the actual helicopter pilot met with the committee.

On a different topic, Joe DeVries raised the issue of an illegal dumping camera pilot program that staff would like to bring forward to the commission for consideration in August. He briefly explained the current illegal dumping ordinance and the fact that the City Council earmarked funding for cameras to enforce the illegal dumping ordinance several months ago and the contracting process for that may be closing soon.

Member Suleiman raised a concern about SFPD sending investigators into Muslim Community Centers fishing for information. She asked if this sort of tactic would be the type of tactic the Commission will be discussing. Vice Chair Brown felt that it would be suitable to discuss. Member Karamooz noted it may depend on whether the information collected gets digitized and then shared (versus just staying within the purview of the individual investigator).

Last, Chairperson Hofer noted that the City has a Cellphone Site Simulator Policy that will be going to the Public Safety Committee in the fall that they would like to first bring forward to the Commission. This can be discussed at the August meeting.

7. 6:45pm: Open Forum

Allan Brill, a former member of the DAC Ad Hoc Committee expressed his gratitude for seeing the Commission created and the people volunteering their time to serve on the Commission. He is the

Chair of his Neighborhood Crime Prevention Council and is very interested in building trust among and between the neighbors and police and sees how surveillance can sometimes undermine that trust. In his neighborhood many people have installed private cameras that surveil public spaces ad many people do not know what is appropriate. He is looking to the Commission to help develop some standards that neighborhoods can embrace.

8. 7:00pm: Adjournment

The meeting adjourned at 7:30pm.

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: July 15, 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; 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. 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.

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 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

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; 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 collect 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; 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

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**
Captain 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

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 or 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 not 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.

The cellular site simulator will not 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 (fire, earthquake, flood)
~~(c)~~(d) Assist in investigations involving danger to the life or physical safety of an invidual
~~(d)~~(e) Apprehend fugitives

XXX.5.1LEGAL 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.

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.

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.

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) A list The number of times that agencies other than the Oakland Police Department that 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. [DA1]

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:

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

A record of destruction shall be recorded. [PA2]

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

Document Overview

The purpose of this document is propose a methodology for assessing every surveillance technology initiative that is contemplated by the City of Oakland in a consistent, objective, and transparent manner. It is intended that this framework will be augmented and improved each time the Privacy Advisory Commission (PAC) evaluated surveillance technology.

PAC expects that each initiative submit its completed Surveillance Technology Assessment Questionnaire (STAQ) to e PAC with sufficient time to review the material in advance of the agendized item date, but no less than four weeks in advance.

Questionnaire

	Question	Response	Supporting Documentation
1	**Why: Initiative Overview**		
1.1	What is the underlying problem targeted to be solved by the overall initiative?		
1.2	What is the quantifiable expected contribution of the envisioned surveillance technology to achieving the solution?		
1.3	What evidence exists to support the expected contribution of envisioned surveillance technology to achieving the solution?		
1.4	What non-surveillance alternative were considered?		
1.5	Why were the non-surveillance technology options not pursued?		
2	**What: Surveillance Technology Detail**		
2.1	How Does the technology work?		
2.2	What else can the technology do that is not intended for deployment?		
2.3	What safeguards, monitors, and audits will		

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

	Question	Response	Supporting Documentation
	be implemented to ensure that non-functioning components of the technology are not activated without proper authorization?		
2.4	What information does the technology capture?		
2.5	What information does the technology store?		
2.6	How long with the stored information be stored?		
2.7	What is the process for destroying information stored on the system?		
3	**Who: Authorized Users**		
3.1	Who is authorized to access the technology?		
3.2	How are authorized users authenticated?		
3.3	How is access to the technology logged?		
3.4	What is the mechanism for monitoring compliance with access policies?		
4	**Where: Location(s) of deployment and data storage**		
4.1	Where would the technology be deployed within the community?		
4.2	What is the basis for selecting these locations?		
4.3	What are the crime statistics for each proposed deployment location?		
4.4	Where will the information be stored?		
4.5	What are the safeguards, monitors, and audits to		

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

	Question	Response	Supporting Documentation
	ensure security of information at storage site (at rest) and when accessed (transmission)?		
5	**How: Protecting Civil Rights and Liberties**		
5.1	Could the technology collect information related to race, citizenship status, gender, age, socioeconomic level, reproductive choices, or sexual orientation? If so, what safeguards are in place to limit such collection?		
5.2	Would the technology be deployed in communities with minority residents, non-citizens, low-income residents, or any group historically vulnerable to disproportionate civil liberties violations?		
5.3	Could the technology be used on groups, public gatherings, or crowds and thus have an effect on First Amendment activities such as protests? If so, what safeguards are in place to limit this?		
5.4	Does the technology collect and retain information about individuals who are not subjects of any criminal investigation? If so, how could such information impact those persons' right to privacy?		
6	**How Much: Initial and On-going Costs of Technology**		
6.1	What are the initial costs,		

City of Oakland
Privacy Advisory Commission
Surveillance Technology Assessment Questionnaire (STAQ)

	Question	Response	Supporting Documentation
	including acquisition, infrastructure upgrades and training and hiring of personnel?		
6.2	What are the ongoing costs, including measures to secure data and data storage?		
6.3	What are the current or potential sources of funding?		
6.4	Are there other tools capable of furthering the identified purpose that the community may wish to spend these funds on (e.g., community-based policing, improved lighting)?		

The [Council/Board of Supervisors] finds that any decision to use surveillance technology must be judiciously balanced with the need to protect civil rights and civil liberties, including privacy and free expression, and the costs to [City/County]. The [Council/Board] finds that proper transparency, oversight and accountability are fundamental to minimizing the risks posed by surveillance technologies. The [Council/Board] finds it essential to have an informed public debate as early as possible about whether to adopt surveillance technology. The [Council/Board] finds it necessary that legally enforceable safeguards be in place to protect civil liberties and civil rights before any surveillance technology is deployed. The [Council/Board] finds that if surveillance technology is approved, there must be continued oversight and annual evaluation to ensure that safeguards are being followed and that the surveillance technology's benefits outweigh its costs.

Comment [Y1]: What do you think of adding more prefatory/whereas language about the value of privacy, the potentials and possible pitfalls of new technologies, the history of this issue and importance to Oakland, and so on? I can help draft something if you think it makes sense.

NOW, THEREFORE, BE IT RESOLVED that the [Council/Board] of [City/County] adopts the following:

Section 1. Title

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

Section 2. [Council/Board] Approval Requirement

1) A [City/County] entity must obtain [Council/Board] approval at a properly-noticed 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 [Council/Board]; or
    d) Entering into an agreement with a non-[City/County] entity to acquire, share or otherwise use surveillance technology or the information it provides.
2) A [City/County] entity must obtain [Council/Board] 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/County] entity seeking approval under Section 2 shall submit to the [Council/Board] a Surveillance Impact Report and a proposed Surveillance Use Policy at least forty-five (45) days prior to the public hearing.
2) The [Council/Board] shall publicly release in print and online the Surveillance Impact Report and proposed Surveillance Use Policy at least thirty (30) days prior to the public hearing.

Section 4. Determination by [Council/Board] that Benefits Outweigh Costs and Concerns

The [Council/Board] shall only approve any action described in Section 2, subsection (1) of this ordinance after making a determination that the benefits to the community of the surveillance technology outweigh the costs; ~~and~~ that the proposal will safeguard civil liberties and civil rights; and that, in the 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/County] entity possessing or using surveillance technology prior to the effective date of this ordinance shall submit a proposed Surveillance Use Policy no later than ninety (90) days following the effective date of this ordinance for review and approval by [Council/Board]. If such review and approval has not occurred within sixty (60) days of the submission date, the [City/County] entity shall cease its use of the surveillance technology until such review and approval occurs.

Section 6. Oversight Following [Council/Board] Approval

1) A [City/County] entity which obtained approval for the use of surveillance technology must submit a Surveillance Report for each such surveillance technology to the [Council/Board] within twelve (12) months of [Council/Board] approval and annually thereafter on or before November 1.
2) Based upon information provided in the Surveillance Report, the [Council/Board] shall determine whether the benefits to the community of the surveillance technology outweigh the costs and civil liberties and civil rights are safeguarded. If the benefits do not outweigh the costs or civil rights and civil liberties are not safeguarded, the [Council/Board] shall direct that use of the surveillance technology cease and/or require modifications to the Surveillance Use Policy that will resolve the above concerns.
3) No later than January 15 of each year, the [Council/Board] 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 [Council/Board] approval pursuant to Section 2 or Section 5, including whether the [Council/Board] 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;
    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. A summary of community complaints or concerns about the surveillance technology;
    d. The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;
    e. Information, including crime statistics, that help the community assess whether the surveillance technology has been effective at achieving its identified purposes;
    f. Statistics and information about public records act requests, including response rates; and
    g. 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.
2) "[City/County] entity" means any department, bureau, division, or unit of the [City/County].
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 or similar information specifically associated with, or capable of being associated with, any individual or group.

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

a. **Description:** ~~(a)~~ Information describing the surveillance technology and how it works, including product descriptions from manufacturers;

b. **Purpose:** ~~(b)~~ information on the proposed purposes(s) for the surveillance technology;

c. **Location:** ~~(c)~~ the location(s) it may be deployed and crime statistics for any location(s);

d. **Impact:** ~~(d)~~ an assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public; ~~and~~

e. **Fiscal Cost:** ~~(e)~~ the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;

f. **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;

g. **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,

h. **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).

~~4)~~

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 uses that are authorized, 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.

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/County] or non-[City/County] 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.

Formatted

Comment [Y2]: I know the next section discusses third-parties, but I believe Section 5 is mainly focused on third-parties like other law enforcement agencies with whom data is shared. This proposed addition is mainly to better understand at the outset who is handling the data on a day-to-day basis.

Formatted: Font: (Default) Times New Roman

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

Section 8. Enforcement

1) 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 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, 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.

~~1)~~

3) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought ~~to enforce this Ordinance~~under paragraphs (1) and (2).

~~2)~~

~~3)~~4) In addition, for a willful, intentional, or reckless violation of this Ordinance or of a Surveillance Use Policy, an individual shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding $1,000 per violation~~, imprisonment in the county jail for not more than six months, or both such a fine and imprisonment~~.

Section 9. 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 10. Effective Date

This Ordinance shall take effect on [DATE].

Comment [Y3]: One - It is unclear who can be sued under this ordinance. Can you sue the city for any violation? Can you sue the agency? Can you sue the agency head? Do you sue the individual agent or city employee who committed the violation? I would support clarifying this.

Two – It is unclear whether a "violation of this Ordinance" is limited to procedural violations (not going through the required surveillance impact report process) or whether it includes violations of a particular technology's surveillance use policy (retention of data beyond the authorized period of time, use of data beyond authorized purpose, etc.). I would support making explicit in this Section that you can sue to enforce a Use Policy.

Formatted: Font: (Default) Times New Roman

Formatted: Font: (Default) Times New Roman

Comment [Y4]: I think there should be room for both individual liability and municipal liability in damages. However, I am not sure whether the standard for the city should be strict liability (all violations by employees) or whether it should be limited to situations in which the city itself engaged in wrongdoing (ie, there was a policy/practice/custom of violating the ordinance/use policy; a high-level policymaker endorsed or ratified the conduct; and so on—similar to *Monell* standards but perhaps not quite as demanding). I think it's something we may want to discuss and hear perspectives from the city about. Strict liability seems attractive and create an incentive for good internal oversight and control, but at the same time there might be individual wrongdoers the city can't do anything about.

Comment [Y5]: This is the liquidated damages formula in FISA (50 USC Sec. 1810)

Comment [Y6]: Should we add something to the Ordinance that discusses the duty of care third-party vendors who are contracted to store or secure data collected through city technologies have to keep it secure? I can seek input from some of my colleagues who practice in this area if you think it's worth exploring.

Formatted: Font: (Default) Times New Roman

Comment [Y7]: I have serious qualms about including a prison term for a violation of this ordinance. I don't think it's inline with our city's decriminalization attitude and I find it highly unlikely a DA would prosecute someone for violations of the ordinance. I would rathe ... [1]

Page 4: [1] Comment [Y7] **Yaman** **8/1/2016 4:03:00 PM**

I have serious qualms about including a prison term for a violation of this ordinance. I don't think it's inline with our city's decriminalization attitude and I find it highly unlikely a DA would prosecute someone for violations of the ordinance. I would rather beef up civil, private enforcement. What do you think?