DAC Privacy and Data Storage Policy Meeting
November 15th, 2013
Building Bridges Room, City Hall

| Item | Time | Outcome |
|---|---|---|
| Review proposed policy framework and mission statement for the DAC | 1-1:40 | Group will review attached policy framework |
| Discuss timeline for presenting to Council and ACLU | 1:40-2:00 | Group will decide on when to meet with City Council (unofficially) and ACLU or other outside interests. |
| Work plan Discussion | 2:00-2:30 | Group will decide who will draft the policy, contact the Port, contact other agencies, and draft personnel policies. |

Proposed framework:

1. The DAC will only retain data for ***(one day, ~~one week, or one month?~~)*** except when an incident is recorded by the monitoring team. Anytime an incident is recorded, the normal data retention policies of the agency (OPD, OFD, Port) will go into affect.
2. The DAC will not attempt to store data recorded by outside camera systems nor will the City attempt to require outside systems to modify their data storage and retention policies. If a private system wishes to connect to the DAC, it's data will only be stored if an incident is recorded.
3. If the City provides funding for the purchase and installation of any private or quasi-public video surveillance system that is connected to the DAC, the only data storage requirement that the city will impose is that the owner/operator provide access to the footage for the city when there is a recorded incident or major crime in the area. If the private system wishes to retain data for any length of time, the data will not be subject to the City's policies nor considered public and therefore not subject to FOIA requests.
4. Only public employees of the City of Oakland will be used to monitor the DAC, no private contractors will be allowed to serve in that role. All employees who are assigned to monitor the DAC will be required to undergo specific training around constitutional rights, protections, and appropriate uses of the surveillance system.
5. A disciplinary policy that is within the Civil Service Rules will be developed and implemented to ensure monitors are not mis-using the system.
6. Periodical audits of the surveillance monitoring will be conducted by supervisorial staff to ensure compliance with the policies and procedures that are implemented.
7. ~~Quarterly~~ Annual Random sampling of stored data will be reviewed by the City Auditor's Office to ensure compliance.

* Annual Performance Audits will be conducted by City Auditor.

DAC Privacy and Data Storage Policy Meeting
December 13th, 2013
Building Bridges Room, City Hall

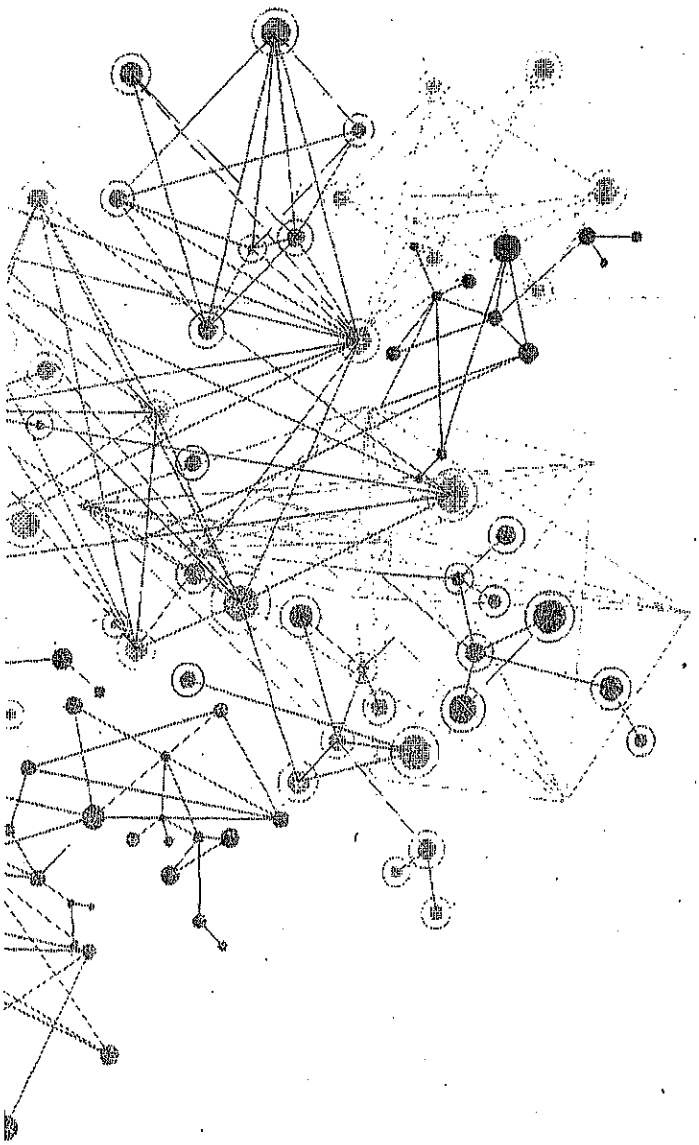
| Item | Time | Outcome |
|---|---|---|
| Introductions | 3:30-3:40 | |
| Review proposed policy framework and mission statement for the DAC | 3:40-4:00 | Group will review below policy framework. |
| Discuss State Data Retention Standards | 4:00-4:15 | Group will discuss possible obstacles caused by state law to a short data storage retention policy. |
| Discuss next steps, next meeting. | 4:15-4:30 | |

Proposed framework:

1. The DAC will only retain data for 72 hours except when an incident is recorded by the monitoring team. Anytime an incident is recorded, the normal data retention policies of the agency (OPD, OFD, Port) will go into affect.
2. The DAC will not attempt to store data recorded by outside camera systems (beyond 72 hours) nor will the City attempt to require outside systems to modify their data storage and retention policies. If a private system wishes to connect to the DAC, its data will only be stored if an incident is recorded.
3. If the City provides funding for the purchase and installation of any private or quasi-public video surveillance system that is connected to the DAC, the only data storage requirement that the city will impose is that the owner/operator provide access to the footage for the city when there is a recorded incident or major crime in the area. If the private system wishes to retain data for any length of time, the data will not be subject to the City's policies nor considered public and therefore not subject to ~~FOIA~~ requests. PRA.
4. A disciplinary policy will be developed and implemented to ensure monitors are not using the data inappropriately.
5. Periodical audits of the surveillance monitoring will be conducted by supervisorial staff to ensure compliance with the policies and procedures that area implemented.
6. Reviews by the City Auditor's Office to ensure compliance will be conducted on a regular basis (quarterly, annual).

Take OAP. Job Appropriate, calls and or Case Approval.

# VI. FUSION CENTER RECOMMENDATIONS



## A. Data Collection Recommendations

### Profiling and Data Collection:

1. Fusion centers should establish guidelines that clearly prohibit their personnel from engaging in racial and religious profiling. In determining when to collect and share information, the guidelines should focus on behaviors that raise a reasonable suspicion of criminal activity or evidence of wrongdoing. Race, national origin, ethnicity and religious belief should not be considered as factors that create suspicion, and should only be used as factors in alerts if they are included as part of a specific suspect's description. The guidelines should also specify that political association and the peaceful exercise of constitutionally protected rights may not be relied upon as factors that create suspicion of wrongdoing.
2. Fusion centers should ensure that their personnel are properly trained on the constitutional rights of free expression, assembly, religion and equal protection.
3. Fusion centers should ensure that individuals who instruct their personnel on intelligence analysis and terrorist threats are competent and well-qualified, and have themselves been trained in the constitutional rights discussed above.

### Suspicious Activity Reporting:

4. Fusion centers should carefully analyze suspicious activity reports to determine whether there is a likely connection to criminal or terrorist activity, and should only retain and disseminate suspicious activity reports if they demonstrate reasonable suspicion of such activity.

## B. Data Storage and Use Recommendations

### Data Minimization:

1. Fusion centers should periodically review the information in their files to determine whether that information is accurate and of continuing relevance. Data retained by fusion centers should be purged five years after its collection unless its continued relevance can be demonstrated.
2. Fusion centers should collect and retain only the minimum amount of personally identifiable information necessary to

serve their law enforcement purposes. Fusion centers should only use this personally identifiable information for the law enforcement purpose for which the information was collected.

**Audit Logs:**

3. Fusion centers should ensure that immutable audit logs track all database activity.
4. Independent auditors should review fusion center audit logs every two years and publish reports describing the use of fusion center databases and any abuses or unauthorized access.

**Data Mining:**

5. As set forth in The Constitution Project's report *Principles for Government Data Mining*, fusion centers should act carefully to ensure that constitutional rights and values are respected if they engage in data mining or if the information in their databases is used for data mining by other government entities.

**Private Sector Partnerships:**

6. Fusion centers should carefully limit the information that they disseminate to private sector entities. Personally identifiable information should only be shared with private sector entities to the extent necessary to carry out legitimate law enforcement or national security functions.
7. Fusion centers should not collect information from private sector sources that they would otherwise be restricted by law from obtaining.

## C. Accountability Recommendations

**Mission Statement:**

1. Fusion centers should develop clear mission statements that express their purpose and the criteria upon which their performance can be evaluated. Further study of the proper goals and methods of fusion centers would be useful for the development of these mission statements and accountability criteria.

**Transparency:**

2. Fusion centers should engage local communities by publicly explaining their mission, budget and staffing.
3. Fusion centers should publicize their privacy policies and the results of their compliance audits.

**Redress:**

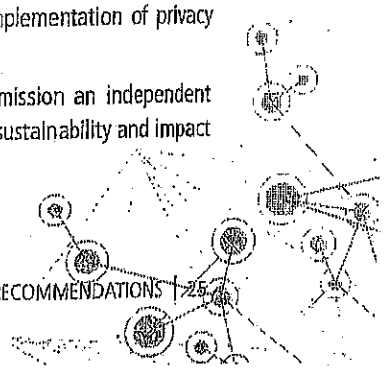
4. Fusion Centers should be equipped with effective redress processes by which individuals can, if necessary, review and correct or challenge information possessed by a fusion center.
5. Redress processes should provide for the availability, where appropriate, for review of complaints by an independent, security-cleared arbiter, with a right of appeal to a higher-level independent state or local authority.
6. Redress processes should be well-publicized.
7. Redress processes should ensure that corrections are disseminated across databases.

**State Oversight:**

8. State governments should ensure that fusion centers are subject to state privacy, open government and anti-domestic surveillance laws, regardless of federal pressure to the contrary.
9. States should require periodic audits of fusion center privacy practices and that fusion centers privacy practices be subject to review by an oversight board or officer.

**Federal Guidance and Oversight:**

10. The federal government should regularly audit fusion centers for compliance with privacy guidelines and report its findings to the appropriate congressional committee of jurisdiction.
11. Federal funding for fusion centers should be separate and distinguishable from general funding for state and local law enforcement activities.
12. Federal funding for fusion centers should be contingent upon:
    a. States enacting legislation that (i) subjects fusion centers to periodic state audits of their civil liberties practices, and (ii) requires fusion centers to comply with state privacy, open government and anti-domestic surveillance laws; and
    b. Continued compliance with federal and state privacy and civil liberties guidelines, as assessed by periodic federal audits.
13. The federal government should provide fusion centers with increased civil liberties training and detailed and specific guidance regarding the practical implementation of privacy protections.
14. Congress, DHS or DOJ should commission an independent study of fusion center performance, sustainability and impact upon civil liberties.



[redacted]

1/23/14

City of Oakland

Policy on Recording and Data Retention for Domain Awareness Center

I. Background and Overview

*[Brief description of what the Domain Awareness Center is]*

II. Purpose/Mission Statement

III. Policy updates

This Privacy and Data Retention Policy Framework is developed as a working document, and will be periodically updated to ensure the relevance of policy with the ever changing field of technology. The fundamental purpose of this policy is to protect the privacy of the general public and erect safeguards around any data captured and retained by the DAC, against improper use and/or distribution.

~~III.~~IV. Definitions

"DAC data' means . . .

"Emergency" means the existence of conditions of disaster or extreme peril to the safety of persons and property within the territorial limits of the City of Oakland or having a significant adverse impact within the territorial limits of the City of Oakland, caused by such conditions as air pollution, fire, flood, storm, epidemic, riot, drought, sudden and severe energy shortage, plant or animal infestation or disease, the state Governor's warning of an earthquake or volcanic prediction, or an earthquake, or other conditions, which are likely to be beyond the control of the services, personnel, equipment, and facilities of the City of Oakland and require the combined forces of other political subdivisions to combat, or with respect to regulated energy utilities, a sudden and severe energy shortage requires extraordinary measures beyond the authority vested in the California Public Utilities Commission.

[redacted]

Formatted: Underline

Formatted: Indent: Left: 0.5", No bullets or numbering

Formatted: Indent: Left: 0.25"

Formatted: Underline

Formatted: Normal, No bullets or numbering

[redacted]

"Incident means" an occurrence or event, natural or human caused, that requires an emergency response.

"Operator" means

~~IV.~~V. Technological Capabilities

~~Description of the DAC's current and proposed (up to Phase 2 build-out) operational capabilities~~

**Analytics, such as facial and gait recognition software:**

1. No analytics are planned that would use biometric data to identify individuals.
2. Analytics are in use to identify significant security events. Examples:
   a. Crossing of fence lines from public areas into secured areas
   b. Unusual activity within secured areas
   c. Object sensors that identify vehicles traveling far above the speed limit, which are used to alert for drag racing at the Port.
3. Future uses of analytics could likely include further alerts to enhance public safety. Examples:
   a. Large container ships traveling at high speeds toward bridge supports.
   b. Large trucks parked in unauthorized areas

**License Plate Readers:**

License Plate Readers (LPR's) are used to raise alerts of license plates that are on a "hot list". The DAC does not receive or database LPR data directly, but will receive alerts from systems that process LPR data.

**Shot Spotter:**

The DAC receives Shot Spotter alerts from the system provider in pre-parsed and packaged form. The DAC does not receive raw data streams from Shot Spotter sensors. Alerts that match pre-determined criteria are stored in the DAC system as events.

**Social Media:**

The DAC does not currently have privileged access agreements with any social media provider. Privacy of social media data is controlled by each individual social media provider. Social media could be accessed by the DAC via the same methods available to the public. Individual operators of the DAC could also potentially access social media using their own means according to that individual's employment agreement, HR policy or other applicable policy.

[redacted]

[redacted]

Formatted: Indent: First line: 0.5"

Formatted: Indent: Left: 0.5"

Formatted: Indent: First line: 0.5"

Formatted: Indent: Left: 0.5"

Formatted: Indent: First line: 0.5"

Formatted: Indent: Left: 0.5"

Formatted: Indent: Left: 1", No bullets or numbering

~~V.~~VI. Access to the DAC system/equipment

For live monitoring (Supervisor and staff hired for day to day operations)

Only ~~public employees of the~~ City of Oakland (employees) will be used to monitor any data systems or camera feeds that will come into the DAC, no private contractors will be allowed to serve in that role. All employees who are assigned to monitor the data systems and camera feeds that will come into the DAC will be required to undergo security background checks at the local level as well as security clearances at state and/or federal levels to ensure data and information security. Also, all employees will be required to participate in specific training around constitutional rights, protections, and appropriate uses of the data systems and the camera surveillance system.

Critical incidents/emergencies/EOC activations

During a major emergency EOC key staff and key outside agencies that would report to EOC also DAC staff

For maintenance

DIT and vendors that installed systems as well as other maintenance providers

For other purposes you envision

When system is not live, Delegations that come for visits to Tour EOC

When DAC or EOC is not live, or DAC function is moved to Port side room for DAC operations; Other staff and outside participants for EOC training

For Audits.

3rd party Auditor, grantor auditors or City Auditor

Any relevant exceptions
TBD

~~VI.~~VII. Access to information and data obtained through DAC

Only City employees with a need to know or right to know will have access to the data gathered by the DAC. Other than staff at the DAC, any sworn or non-sworn personnel without a direct role in investigating an incident will not be permitted access to DAC data.

Formatted: Font color: Auto
Formatted: Indent: First line: 0.04"
Formatted: Font: (Default) Arial, 10 pt
Formatted: Font color: Auto
Formatted: Indent: First line: 0"
Formatted: Font color: Auto
Formatted: Font color: Auto
Formatted: Font color: Auto

Periodic audits of any and all surveillance monitoring will be conducted by the program manager to ensure compliance with the policies and procedures that are implemented.

Annual Performance Audits will be conducted by the City Auditor or outside Auditor.

~~VII.~~VIII. Use Restrictions

General restrictions

- Under no circumstances shall the DAC be used for the purpose of infringing upon First Amendment rights. Operators of the DAC shall not target or observe individuals solely based on their race, gender, sexual orientation, disability or other classifications protected by law. The City shall not "track" the movement of an individual(s) by using DAC system unless there is a reasonable suspicion of criminal ~~wrongdoing~~ activity.

Surveillance Video Camera Use

- The City shall not use audio in conjunction with closed circuit television cameras unless appropriate court orders are obtained.
- Operators shall abide by the restrictions set forth in this policy regardless of the sources of the closed circuit television video feeds.
- Closed circuit television systems shall only be used to observe locations that are in public view and where there is no reasonable expectation of privacy.
- The City will only add additional cameras to feed into the DAC upon the approval of the City Council.
- Operators shall not focus on hand bills, fliers, etc., being distributed or carried pursuant to First Amendment rights.

Data storage

Pursuant to Government Code Section 34090 the City will retain any recorded data for two years except when an incident or emergency is recorded by DAC monitoring staff at which point the data retention policies of the agency that has conducted the monitoring will apply (OPD, OFD, Port). In the case of data recorded by OPD, such data will be retained as evidence based on the time periods specified by State Law based on statute code.

The DAC will not attempt to store (record) data received from outside camera systems except when those systems have no recording capability, nor will the City attempt to require outside systems to modify their data storage and retention policies. If a private system wishes to connect to the DAC, its data will only be stored if an incident that is captured by that feeder system is recorded.

[redacted]

Formatted: Indent: First line: 0.5"

Formatted: Normal, Indent: First line: 0.25", No bullets or numbering

Private Cameras none are linked in sept will only be linked in w/ Council Approval.

If the City provides funding for the purchase and installation of any private or quasi-public video surveillance system that is connected to the DAC, the only data storage requirement that the city will impose is that the owner/operator provide access to the footage for the city when there is a recorded incident or major crime in the area. If the private system wishes to retain data for any length of time, the data will not be subject to the City's policies.

Comment [d12]: Do we want to say this??? Are we looking at purchasing and installing private video systems? Should we define this more clearly?? Just a question and food for thought.

"Secondary" use of data / Info. Sharing Follow own Section?

- Is this envisioned?
- If so, what safeguards should be in place (ie supervisor/commander's approval)
- What about release of information to 3rd parties?

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.75" + Indent at: 1"

Formatted: Superscript

Formatted: Font: Calibri

Formatted: List Paragraph, Indent: Left: 1"

~~VIII.~~IX. Locations of Closed Circuit Cameras

a. City of Oakland

i. Public Notice

ii. Specific Locations

Closed Circuit Television Cameras that feed into the DAC are located at the following places in the City of Oakland:

*[We need a list of camera locations]*

b. Port of Oakland

~~IX.~~X. Audits

a. Program Manager

*Periodic* audits of the surveillance monitoring will be conducted by the program manager to ensure compliance with this policy.

b. City Auditor

Annual performance audits will be conducted by the City Auditor's Office to ensure compliance with this policy. These audits shall be provided to the Mayor, City Administrator, and City Council at least *[fill in time frame]* .

XI. Records Management

- Who will be the DAC custodian of records?
- Considering the background checks, privacy issues, etc.,
- Who will be the PRR liaison for DAC records?
- Who will be redacting records?

Formatted: Indent: Left: 0.5", No bullets or numbering

Formatted: Normal, Indent: First line: 0.5", No bullets or numbering

What kind of equipment is available to redact records, and who will have access to it?

To how many positions will the DAC project provide funding to respond to PRR's?

~~X.~~

Formatted: Normal, No bullets or numbering

~~XI.~~XII. Redress and Public Information Requests

a. The Public's Access to Video Recordings
For recorded images fed into the DAC, Individuals may request a copy of such records by contacting [insert the department who will be the custodian of records, i.e. Fire Dept.].

b. Individuals who request a copy of recorded images of themselves must provide details to allow the City to identify them as them as the subjects recorded images. Such a request should include the location, time, and date of recorded images.

~~XII.~~XIII. Sanctions and Enforcement Remedies

Advisory Panel.