

|



REPORT

AGENDA

TO: JOHN A. FLORES
INTERIM CITY ADMINISTRATOR

FROM: Joe DeVries

SUBJECT: DAC Privacy and Data Retention Policy

DATE: January 28, 2015

City Administrator
Approval

Date

COUNCIL DISTRICT: City-Wide

RECOMMENDATION

Staff recommends that Council:

1. Accept this Report and adopt a Resolution: 1) affirming the right to privacy; 2) establishing the City of Oakland Domain Awareness Center (DAC) privacy and data retention policy which prescribes the rules for the use, accessing and sharing of DAC data; establishes oversight, auditing and reporting requirements; and imposes penalties for violations; and 3) authorizing the DAC to become operational
2. Consider additional policy recommendations which require future Council action from the DAC Ad Hoc Advisory Committee that will support the policy, assure ongoing compliance with the policy, establish penalties for violation of the policy, and potentially extend the components of the Policy to a broader range of City functions.

EXECUTIVE SUMMARY

The DAC Ad Hoc Advisory Committee developed this Privacy and Data Retention Policy, hereafter referred to as “the Policy” (Resolution, Attachment A) at Council’s direction contained in Resolution No. 84869 C.M.S. which stated that “A data retention as well as a privacy policy shall be developed by the Council Approved Advisory Body prior to the activation of the Port-only Domain Awareness Center. The attached resolution affirms the City Council’s direction and adopts the draft Policy as official City Policy.

Item: _____
Public Safety Committee
February 10, 2015

Staff also requests that Council consider the accompanying recommendations for future council action from the Ad Hoc Advisory Committee, some of which are outside the authority of the Advisory Committee but still relevant to the work of that body. These recommendations either support the Policy or further its purpose to encompass future City Technology:

1. Establish a Standing Privacy Policy Advisory Committee of the City to provide guidance to the City Council on potential changes to either the DAC or the DAC Privacy and Data Retention Policy.
2. Recommend to the City Administrator that a person is designated and shall serve as the Internal Privacy Officer within the DAC charged with ensuring the DAC Staff are abiding by the Policy, and that the City Auditor shall serve as the "Compliance Officer" who is responsible for reviewing the quarterly reports prepared by the Internal Privacy Officer, and that the Public Ethics Commission shall serve as an Ombudsman/Advocate to receive complaints from whistleblowers or the general public and to make policy recommendations to the Advisory Committee and City Council.
3. Request the City Administrator or designee prepare an ordinance that makes violation of the Policy a misdemeanor punishable by fines and also enforceable by injured parties under a private right of action.
4. Determine that changes must be proposed by/to the Privacy Advisory Committee and ratified by the City Council and that Privacy policy must be reviewed at least every year by the committee.
5. Create a Permanent Standing Advisory Committee to examine the City as a whole and develop an overarching Privacy Policy that would reach beyond the limited scope of the DAC.
6. Modify the City's Whistleblower Ordinance to broaden protections and allow for more avenues to file a complaint when there is a DAC policy related potential violation.
7. Consider establishing a Citywide Surveillance Technology Ordinance to allow for informed public debate and decision making by the City Council regarding privacy and retention policies for all Surveillance Technologies in the future.

The attached Draft Policy is almost completely the product of the Ad Hoc Advisory Committee with the exception of three modifications that occurred after the last meeting of the committee. Those modifications are supported by the City Administrator and are as follows:

- On page one, a sentence that stated "*Therefore, the DAC and the entirety of this policy are exclusive to Port areas within Oakland*" was removed at the request of the Port because it was duplicative and because there was concern it would confuse the reader to assume the Policy covered internal Port operations which it does not.

Also on page one, the last sentence of the Policy Purpose Section states, "*Notwithstanding any other language or statement contained herein, this Policy shall be limited to the actual activation of the joint City-Port DAC at the EOC located 1605*

Item: _____
Public Safety Committee
February 10, 2015

Martin Luther King Jr. Way, in Oakland, California by City staff whether acting solely or in conjunction with Port staff. Further this Policy does not prohibit the Port from monitoring Port properties by using security systems solely operated by the Port and outside of the City's control."

- This sentence was added to provide clarity for the reader that the DAC is located at the Emergency Operations Center (EOC) located at 1605 Martin Luther King Jr. Way, in Oakland, California and not at the Port of Oakland. This Policy does not apply to the Port's operation of its own security systems that the City has no control over and that are not housed at the EOC.
- The City Attorney has reviewed the language presented to the City extensively and, to add clarification, has recommended that the following paragraph be added to the policy on page 2 as the last paragraph of the Policy Purpose Section: *Notwithstanding the provisions of this policy, the City does not waive any right as provided by any relevant federal, state, or local law including but not limited to the California Public Records Act and the California Emergency Services Act. Further, the provisions of this policy do not relieve the City of any existing responsibilities, duties, or obligations as provided by any Memorandum of Understanding or Agreement for which the City is a party or any local, state, or federal law. Finally, nothing in this policy is intended to prohibit the DAC from being used as specified in Section VII.B or is intended to create a new privacy right for individuals beyond what is protected by the California and United States Constitutions.*

OUTCOME

Adoption of the Policy will satisfy the Council direction provided to staff on March 4, 2014 via City Council Resolution No. 84869 C.M.S. ensuring the development of a "Privacy and Data Retention Policy for the Domain Awareness Center (DAC)" before the DAC is made operational. This policy's purpose is to protect the Right to Privacy, civil liberties, and freedom of speech of the general public as well as erect safeguards around any data captured at the DAC when activated, and to protect against its improper use, distribution, and/or breach.

Adoption of **recommendations 1-4** from the Ad Hoc Advisory Committee above are directly related to portions of the Policy that cannot be enabled without further Council action including establishing enforceable consequences for violations of the Policy, establishing a reporting and auditing framework, and continuing ongoing citizen review.

Adoption of **recommendation 1**, which would require future Council action, would allow for the creation of a Standing Advisory Committee to oversee the work of the DAC specifically. Council would need to direct staff to prepare an Ordinance that delineates the membership and structure of the Committee per the City Charter, and the membership would not necessarily have the same members as the current Ad Hoc Committee.

Adoption of **recommendation 5** essentially expands the role of the Standing Committee (in recommendation 1) beyond the limited focus of the DAC to examine the City as a whole and provide recommendations to the City Council on a broader array of technology and develop an overarching Privacy Policy.

Adoption of **recommendation 6**, which would require future Council action, is to ensure greater opportunity to report abuses of the DAC Data or System; however, it is not required to make the Policy functional.

Adoption of **recommendation 7**, which would require future Council action, is seeking to make the decision making process regarding Surveillance Technology Citywide more public and thorough and expands the discussion outside the narrow scope of the DAC. It would serve as an opportunity to expand the principals of the attached Policy to a wider array of City functions and establish a more public process by which the decision to use new technology is reached.

BACKGROUND/LEGISLATIVE HISTORY

On March 4, 2014 the City Council adopted Resolution No. 84869 C.M.S. that stated, “A data retention as well as a privacy policy shall be developed by the Council Approved Advisory Body prior to the activation of the Port-only Domain Awareness Center. Members of the Advisory Body will be appointed by each member of the City Council.”

Staff worked directly with the City Council Offices to identify individuals that had an interest in serving on the Ad Hoc Committee with a goal of appointing a balanced group that included people with expertise in areas such as privacy rights, civil liberties, technology, as well as individuals who represent Oakland’s neighborhoods and business community.

The DAC Ad Hoc Privacy and Data Retention Advisory Committee conducted its inaugural meeting on May 1st, 2014. It began its work in an information-gathering stage requesting information from staff about: data security, information sharing agreements with outside agencies, situational capabilities and uses of the DAC in its currently proposed form, as well as further analysis of current data retention policies. While this information gathering occurred, the committee also defined a set of core principles that the policy needed to include.

In July, the Committee applied its core principals to the draft Privacy Policy Framework that staff had developed in the winter of 2013 and began redrafting the policy. The Committee ultimately met 18 times over six months to produce the final draft Policy (**Attachment A**) for Council consideration. The Committee also formulated the aforementioned 6 recommendations for the City Council to consider that will support the policy in varying ways, and one

recommendation to further the purpose of the Policy to a broader spectrum of future City Technology.

Prior Council action did not commit any operational funding to the DAC for any type of staffing plan. However, the Port of Oakland previously received and accepted Federal grant funds for the eventual staffing of the first two years of operation of the DAC as it was originally envisioned as a joint City-Port project. Port staff has since examined various staffing scenarios, including a no new City staff option. Based on scope changes to the DAC, including the direction of Council to implement a Port-only approach, and as a result of on-going discussions with the City, the Port Board of Commissioners directed staff to request that Port Security Grant Program (Round 13) funds be reprogrammed to support staffing of existing Port security systems on Port property.

Grant funds will be used to support and manage in-house capabilities at the Port of Oakland has an affirmative obligation under Federal law to continuously monitor its facilities and its approaches on land and water. The Port's Video Monitoring Systems Use Policy will govern use and access to the system.

The DAC Policy will remain intact. However, the DAC system will not be monitored in a continuously active state at the Emergency Operations Center (EOC) by either City or Port staff. Instead, the DAC Policy will only apply if and when the DAC System is activated at the City-owned facility located at Martin Luther King, Jr. Way for any of the many situations identified in Section VIII A of the Policy. Due to this change in anticipated operational use, minor editing changes to the language of the Policy are still required.

ANALYSIS

The creation of the DAC in Oakland, through grant funding from the Department of Homeland Security at a time when the Federal Government's efforts at gathering massive amounts of data about Americans was revealed by Edward Snowden, created a unique local flashpoint in 2013. This serendipitous moment has allowed for a debate to unfold about how Oakland will protect people's civil liberties and personal freedoms in an era of significant expansion of surveillance technology that is designed to more efficiently protect public safety.

The City Council's motion to restrict the scope of the DAC in March of 2014 and create an Ad Hoc Advisory Committee to develop a Privacy and Data Retention Policy has allowed that discussion to unfold in regard to a very practical application. The committee was given a narrow task of developing a policy for a specific technology but the committee members remained conscious throughout the process of the need to be able to apply this policy to a broader array of technologies both currently as well as into the future with technology that has yet to be developed.

Item: _____
Public Safety Committee
February 10, 2015

Therefore, the committee produced a policy that proactively identifies how the technology can be used, how it can be modified, who has oversight over the process, and what course of action should be taken when the policy is violated.

The key points of the Policy include: 1) Data Sharing limitations with outside agencies, 2) Who has a Need and/or Right to the data, 3) Specifically what uses of the DAC are permissible, 4) What is considered “Protected Activity,” 5) How oversight and reporting will occur, and 6) What penalties exists to deter people from violating the Policy. Although the Policy clearly delineates these functions, there is a need for the City Council to make certain determinations that were outside the jurisdiction of the Ad Hoc Committee for the Policy to be enabled. Also, the City Administrator, Public Ethics Commission, and City Auditor would have to make certain determinations for all provisions of the policy to become effective. These are listed below:

1. Establish a Standing Privacy Advisory Committee of the City for the DAC

There are four distinct roles that the Ad Hoc Advisory Committee recommends the City fill to ensure a system of checks and balances exists for the DAC to avoid abuses of the system. The first of which is a Standing Privacy Policy Advisory Committee that would provide guidance to the City Council on potential changes to either the DAC or the DAC Privacy and Data Retention Policy. This committee would also make assessments of new technology that could impact the policy, review annual compliance reports, and provide a venue for public comment. This body’s recommendations would be required before the City Council hears any potential changes to the DAC.

2. Identify the Internal Privacy Officer, Compliance Officer, and Ombudsman/Advocate

The three remaining roles that the Ad Hoc Committee recommends the City identify are recommended as follows:

- a. Internal Privacy Officer: the Committee strongly recommends to the City Administrator that they designate a person to serve as the Internal Privacy Officer within the DAC who is charged with ensuring the DAC Staff are abiding by the Policy on a day-to-day basis. They would be required to check the logs, file reports, and make immediate decisions that arise that do not allow time for a further review. Because the DAC is housed within the EOC, The EOC Manager would be the most likely candidate for this role.
- b. Compliance Officer: The City Auditor or their designee should serve as the “Compliance Officer” who is responsible for reviewing the quarterly reports prepared by the Internal Privacy Officer and should conduct random audits to ensure the DAC Staff is abiding by

the Policy. The committee recommends that the Auditor serve in this capacity as it is synonymous with the Auditor's role as defined in the City Charter.

- c. Ombudsman/Advocate: the Committee recommends that the Public Ethics Commission should serve as an Ombudsman/Advocate. This is recommended to ensure there is an entity outside the City's normal chain-of-command that is both available to receive complaints from whistleblowers or the general public and also to make policy recommendations to the Advisory Committee and City Council. Although this role is not as well fitted as the role the committee identified for the Auditor, it does fit as an outside body that has a degree of authority outside the typical Political or Administrative City functions.

3. *Request the City Administrator or designee prepare an ordinance that makes violation of the Policy a misdemeanor punishable by fines as well as a private right of action by the injured party*

The Committee wrote penalties directly into the Policy to ensure DAC staff would understand the severity of their actions if they were to misuse the data or technology. The Policy currently states that violations are considered a misdemeanor punishable by up to one year in jail or a fine of up to \$1000. This language is compatible with the City Charter requirement that misdemeanor fines are capped at \$1000. In order for this provision to be enforceable, an Ordinance would need to be adopted by the City Council stating so.

The Committee also wanted to acknowledge that when someone's personally identifiable information is misused it is an injury that could ultimately prove very costly therefore; the Committee is recommending that these violations cause the violator to be subject to a Private Right of Action.

Both of these portions of the Policy would require a meet and confer with the City's labor organizations and this process would need to conclude before the full City Council can adopt the Policy.

4. *Changes to the Policy*

Changes must be proposed by staff first to the Privacy Advisory Committee and subsequently ratified by the City Council or the proposed changes should originate *from* the Privacy Advisory Committee and subsequently ratified by the City Council. No changes should be made without this public review process. The Privacy Policy must be reviewed at least every year by the committee.

5. *Create a Permanent Standing Advisory Committee*

The Committee believes the City should establish a Standing Advisory Committee to examine the City as a whole and develop an overarching Privacy Policy that would reach beyond the limited scope of the DAC. This could be the same body as the committee recommended in section 1 but with a much broader purpose. This could also be the entity that develops a Citywide Surveillance Technology Ordinance as recommended below in #8. This body should be sufficiently prepared to consider new technology and compliance with state and federal laws in the ever changing world of data collection and management.

6. *Modification of the City's Whistleblower Ordinance*

The Committee recommends certain modifications to the City's current Whistleblower Ordinance (No. 12890 C.M.S.) that would require future Council action and are as follows:

Amend: 2.38.020 "Whistleblower" defined to include any *person* instead of any *officer or employee* recognizing that retaliation against a contractor or volunteer within the City's organization could stifle whistleblowing:

The current definition:

"Whistleblower" is defined as an officer or employee who reports or otherwise brings to the attention of the City Auditor any information which, if true, would constitute one of the following: a work-related violation by a City officer or employee of any law or regulation; fraud, waste or mismanagement of City assets or resources; gross abuse of authority; a specific and substantial danger to public health or safety due to an act or omission of a City official or employee; or use of a City office, position or resources for personal gain.

The recommended change to the definition:

"Whistleblower" is defined as *any person* who reports or otherwise brings to the attention of the City Auditor *or Public Ethics Commission* any information which, if true, would constitute one of the following: a work-related violation by a City officer or employee of any law or regulation; fraud, waste or mismanagement of City assets or resources; gross abuse of authority; a specific and substantial danger to public health or safety due to an act or omission of a City official or employee; or use of a City office, position or resources for personal gain.

The Committee also recommends the following addition to this section:

Item: _____
Public Safety Committee
February 10, 2015

Any Whistleblower complaint arising from an act governed by the Domain Awareness Center (“DAC”) Privacy and Data Retention Policy may be made to the City Auditor, the Public Ethics Commission, the DAC Privacy Policy Advisory Committee, the DAC Standing Advisory Committee, the DAC Compliance Officer, or the DAC Ombudsman/Advocate.

All other Whistleblower complaints shall be made to the City Auditor.

Any Whistleblower complaint made pursuant to this chapter shall be immediately investigated by the City Auditor or Public Ethics Commission.

This addition would allow for more “doors” through which to file a complaint and draws more eyes to a problem, especially if an employee or other person was uncomfortable coming forward to any particular entity listed.

Amend: 2.38.030 Whistleblower identity

Current Language:

To the extent permitted by law, the identity of anyone reporting information to the City Auditor about an improper government action shall be treated as confidential unless the employee waives his or her confidentiality in writing.

Proposed Language:

To the extent permitted by law, the identity of the *whistleblower* shall be treated as confidential unless the employee waives his or her confidentiality in writing.

This change would simply clean up the old confidentiality section to be more general to ensure that anyone’s identify will be protected regardless of what they are reporting and who they are reporting it to.

The Committee recommends this new section: 2.38.120 Training

All managers, supervisors, and department heads shall undergo periodic training about whistleblower protections, retaliation, and appropriate methods to address employee concerns.

The Committee feels that there needs to be a training of managers and supervisors within the City to ensure they are familiar and compliant with the law.

7. *Citywide Surveillance Technology Ordinance*

The Committee determined that the City of Oakland currently lacks a process that fully informs the public and enables the Council to make an informed decision about the proposal, acquisition, and use of surveillance technologies by City entities. The Committee recommends that the City Council adopt an ordinance that applies to all City entities and provides for at least the following:

Informed public debate and decisions by the City Council about Surveillance Technology

Proposals: Public notice, distribution of information about the proposal, and public debate *prior* to seeking funding or otherwise moving forward with surveillance technology proposals could prove critical to avoiding costly and divisive debates in the future in which the interests of public safety and protection of grant funding is pitted against the interests of full disclosure and civil liberties.

The City Council could facilitate this informed public debate, expressly consider costs (both fiscal and to civil liberties), and determine that surveillance technology is appropriate or not before moving forward with any proposal.

Privacy and Retention Policies for All Surveillance Technologies: Legally enforceable Privacy and Retention Policies with robust civil liberties, civil rights, and oversight safeguards similar to the DAC Policy could be considered and approved by the City Council for each surveillance technology before use.

Ongoing Oversight & Accountability of Its Use: Proper oversight of surveillance technology use and accountability through annual auditing and public reporting and oversight, by the public and the City Council could be required as it is in the DAC Policy.

If the Council does create a Standing Advisory Committee, the Committee's charge could be to begin the process of developing such an ordinance as the first component of its work. This idea is gaining traction throughout the Bay Area and California as more and more cities are wrestling with the increased use of new technologies by law enforcement agencies taking place in a new arena of public policy.

Policymaking bodies have faced challenges keeping up with technological advances that are often funded by federal grant dollars. Local governing bodies, in competing for and accepting grant funding for such technologies, sometimes inadvertently fail to thoroughly and publicly vet the impacts of purchasing and using such technology. A Citywide Surveillance Ordinance could remedy this gap and provide the public with a greater sense of security that their privacy interests are being protected by the City. Throughout the process of developing the DAC Privacy and Data Retention Policy, the Committee Members maintained an understanding that their work could be applied to the City as a whole and the vote to make this recommendation passed unanimously.

PUBLIC OUTREACH/INTEREST

The Ad Hoc Committee was created by Council action due to widespread interest in this issue and an overwhelming outpouring of public speakers when the Council was considering accepting Federal grant funds to finance the construction of the DAC. All meetings of the Committee about the Policy were properly noticed with the City Clerk. Staff also created an email distribution list so that any interested party received all of the agenda materials at the same time as the committee members.

COORDINATION

The City Administrator provided direct staff support to the committee and the following departments also regularly participated and assisted in the preparation for the Advisory Committee Meetings and the Policy those meetings ultimately produced: the Department of Information Technology, City Clerk, City Attorney, Police Department, Fire Department, and the Office of Emergency Services. The City Attorney's Office, the Port of Oakland and Budget Office were consulted in the preparation of the DAC Policy and this report.

COST SUMMARY/IMPLICATIONS

This report has no direct fiscal impact. However, the adoption of some of the recommendations could have a fiscal impact in that they would require staff support on an ongoing basis.

SUSTAINABLE OPPORTUNITIES

Economic: No economic opportunities are identified in this report.

Environmental: No environmental opportunities are identified in this report.

Social Equity: The development and adoption of a privacy policy provides residents with an indication that the City is responding appropriately to concerns about the Domain Awareness Center's impact on residents' civil liberties and is establishing safeguards to prevent potential abuse of the technology or the data collected by the DAC.

For questions regarding this report, please contact Joe DeVries, Assistant to the City Administrator, at (510) 238-3083.

Respectfully submitted,

Joe DeVries,
Assistant to the City Administrator

Attachments:

- A- Final Draft Privacy and Data Retention Policy for the DAC.
- B- Resolution establishing the Domain Awareness Center Privacy and Data Retention Policy