

DAC Ad Hoc Advisory Committee Recommendations to the City of Oakland that supplement and further the Privacy and Data Retention Policy.

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:

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 identity 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.