


City Attorney

FILED
OFFICE OF THE CITY CLERK
OAKLAND

2015 SEP -3 PM 3:11

OAKLAND CITY COUNCIL

RESOLUTION No. _____ C.M.S.

Introduced by Councilmember _____

RESOLUTION ESTABLISHING THE CITY OF OAKLAND’S FORWARD LOOKING INFRARED THERMAL IMAGING CAMERA SYSTEM (FLIR) PRIVACY AND DATA RETENTION POLICY WHICH PRESCRIBES THE RULES FOR THE USE OF THE FLIR; ESTABLISHES OVERSIGHT, AUDITING AND REPORTING REQUIREMENTS; AND IDENTIFIES PENALTIES FOR VIOLATIONS

I. BACKGROUND AND OVERVIEW

WHEREAS, the Law Enforcement Forward Looking Infrared Thermal Imaging Camera System (“FLIR”) was first proposed to the City Council’s Public Safety Committee on March 24, 2015. The purchase of the FLIR will be funded by Federal FY 2014/15 Port Security Grant Program (“PSGP”) monies. The Oakland City Council approved acceptance of the PSGP funds and authorized purchase of the FLIR on April 21, 2015; and

WHEREAS, a thermal imaging camera is a device that forms an image using infrared radiation, similar to a common camera that forms an image using visible light. FLIR technology is commonly used by law enforcement or firefighters when visibility is poor, such as at night, or when smoke is present; and

WHEREAS, in *Kyllo v. United States*, the United States Supreme Court ruled directly on thermal imaging systems, holding that law enforcement must first obtain a warrant when using a FLIR to search a private residence; and

WHEREAS, the Court in *Kyollo* stated: “[w]here, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment ‘search,’ and is presumptively unreasonable without a warrant.” *Kyllo v. US*, (2001) 533 U.S. 27; and

II. POLICY PURPOSE

WHEREAS, this policy’s purpose is to protect the Right to Privacy, civil liberties, and freedom of speech of the general public as protected by the California and Federal Constitutions, and erect safeguards around any data captured and retained by the FLIR, and to protect against its improper use, distribution, and/or breach and in how it is used for law enforcement investigations. This policy shall be referred to as the FLIR Privacy and Data Retention Policy (“Policy”). More specifically, the principal intent of this Policy is to ensure that FLIR use adheres to

constitutionality, especially the 1st and 4th amendments of the U.S. Constitution, and the California Constitution's Article 1. Also, this Policy is designed to see that the FLIR processes are transparent, presume people's innocence, and protect all people's privacy and civil liberties; and

WHEREAS, privacy includes our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, associations, secrets, and identity. The Right to Privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner, and timing of the use of those parts we choose to disclose. The importance of privacy can be illustrated by dividing privacy into three equally significant parts: 1) Secrecy - our ability to keep our opinions known only to those we intend to receive them, without secrecy, people may not discuss affairs with whom they choose, excluding those with whom they do not wish to converse. 2) Anonymity - Secrecy about who is sending and receiving an opinion or message, and 3) Autonomy - Ability to make our own life decisions free from any force that has violated our secrecy or anonymity; and

WHEREAS, this policy is designed to promote a "presumption of privacy" which simply means that individuals do not relinquish their Right to Privacy when they leave private spaces and that as a general rule people do not expect or desire for law enforcement to monitor, record, and/or aggregate their activities without cause or as a consequence of participating in modern society; and

WHEREAS, in adopting this policy, it is not the intent of the City Council to supersede or suspend the functions, duties, and authority of the City to manage and oversee the affairs of the City and to protect public safety. This Policy is intended to affirm the Right to Privacy and freedom of expression, in conformance with and consistent with federal and state law. Nothing in this Policy shall be interpreted as relieving the City's responsibility to comply with any and all labor and union agreements, and to comply with all other City Council applicable policies; and

WHEREAS, for any policy provision that imposes a criminal penalty, creates a private right of action, and/or allows for injunctive relief to be enforceable, Council must first pass an ordinance providing for such remedies; and prior to Council adopting such an ordinance, the City must meet and confer with the affected employee unions; now therefore be it

RESOLVED: That any updates to the policy and to FLIR will be subject to the following:

III. FLIR POLICY DEVELOPMENTS AND UPDATES

A. The City Council shall establish a citywide Permanent Privacy Policy Advisory Committee. The City's Permanent Privacy Policy Advisory Committee shall have jurisdiction as determined by the City Council, including but not limited to reviewing and advising on any proposed changes to this Policy or to the FLIR's technical capabilities or use

B. No changes to this Policy shall occur without City Council approval. This Policy is developed as a working document, and will be periodically updated to ensure the relevance of this Policy with the ever changing field of technology. All changes proposed to this Policy must be submitted to and reviewed and evaluated by the Permanent Privacy Policy Advisory

Committee for recommendation for submission to the City Council, and include an opportunity for public meetings, a public comment period of no fewer than 30 days, and written agency response to these comments. City Council approval shall not occur until after the 30 day public comment period and written agency response period has completed.

C. For any proposed changes for the Policy that occur prior to the City Council establishing the permanent Privacy Policy Advisory Committee, such changes shall be in the purview of the City Council.

D. The requirements and limitations for the FLIR required by City Council Resolution No. 85532 on April 21, 2015, are incorporated herein by reference, as follows:

1: That no information processed by the Law Enforcement Air Unit FLIR Camera will be collected, retained, stored, or disseminated by the Oakland Police Department and the Oakland Fire Department in their use of the Law Enforcement Air Unit FLIR Camera; and be it

2: That the DAC Ad Hoc Committee shall, before the City Council's 2015 summer recess, draft and present a Privacy and Data Retention Policy that specifies the allowable uses of and governs the collection, retention, storage, and dissemination of information processed by the Law Enforcement Air Unit FLIR Camera; and be it

3: That the prohibition on dissemination of information does not include the prohibition of the Oakland Police Department from communicating critical information obtained through the use of the FLIR such as a fleeing suspect's location, to outside agencies assisting in the immediate apprehension of a fleeing suspect who is not inside a private residence;

FURTHER RESOLVED: That the following definitions apply to this policy:

III. DEFINITIONS

“Allowable Use” means the list of uses in Section VI A. of this Policy for which the FLIR can be used.

“FLIR” means a thermal imaging camera that forms an image using infrared radiation, similar to a common camera that forms an image using visible light.

“FLIR Data” means any data, images, or information fed into, stored, collected, or captured by the FLIR, or derived therefrom.

“FLIR Staff” means the City of Oakland police and fire department employees who will be responsible for using the FLIR, including supervisors, and that have completed appropriate training prior to interaction with the FLIR.

“FLIR Vendors” means the various vendors who support and maintain the FLIR.

"ITD" means the City of Oakland's Information Technology Department.

"Need To Know" means even if one has all the necessary official approvals (such as a security clearance) to access the FLIR, one shall not be given access to the FLIR or FLIR Data unless one has a specific need to access the system or data in order to conduct one's official duties in connection with one of the Allowable Uses in Section VIII A. of this Policy. Furthermore, the "need" shall be established prior to access being granted by the designated City official or their designee and shall be recorded in accordance with Internal Recordkeeping requirements under Section IX.

"Personally Identifiable Information" ("PII") means any data or information that alone or together with other information can be tied to an individual with reasonable certainty. This includes, but is not limited to one's name, social security number, physical description, home address, telephone number, other telephone identifiers, education, financial matters, medical history, employment history, photographs of faces, whereabouts, distinguishing marks, license plates, gait, cellphone meta-data, and internet connection meta-data.

"Protected Activity" means all rights including without limitation: speech, associations, conduct, and privacy rights including but not limited to expression, advocacy, association, or participation in expressive conduct to further any political or social opinion or religious belief as protected by the United States Constitution and/or the California Constitution and/or applicable statutes and regulations. The First Amendment does not permit government "to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *White v. Lee* (9th Cir. 2000) 227 F.3d 1214, 1227; *Brandenburg v. Ohio* (1969) 395 U.S. 444, 447.

Example of speech not protected by 1st Amendment: *People v. Rubin* (1979) 96 C.A.3d 968. Defendant Rubin, a national director of the Jewish Defense League, held a press conference in California to protest a planned demonstration by the American Nazi Party to take place in Illinois in five weeks. During his remarks, Rubin stated: "We are offering five hundred dollars . . . to any member of the community . . . who kills, maims, or seriously injures a member of the American Nazi Party. . . . This is not said in jest, we are deadly serious." Rubin was charged with solicitation for murder. The appeals court upheld the charge, reasoning that Rubin's words were sufficiently imminent and likely to produce action on the part of those who heard him. *Id.* at 978-979.

Example of speech protected by 1st Amendment: *Watts v. U.S.* (1969) 394 U.S. 705. The defendant, Watts, stated that he would refuse induction into the armed forces and "if they ever make me carry a rifle the first man I want in my sights is L.B.J." and was federally charged with "knowingly and willfully threatening the president." The Court, reasoned that Watts did not make a "true 'threat'" but instead was merely engaging in a type of political hyperbole. *Id.*, at 708.

"Reasonable Suspicion" means specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch that an individual or organization is involved in a definable criminal activity or enterprise.

Reasonable Suspicion shall not be based on Protected Activity. Furthermore, a suspect's actual or perceived race, national origin, color, creed, age, alienage or citizenship status, gender, sexual orientation, disability, or housing status, shall not be considered as a factor that creates suspicion, and may only be used as identifying information in the description of a criminal suspect.

"Right to Privacy" is recognized by the California Constitution as follows:

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.
Cal. Const. Art. 1, Section 1.

FURTHER RESOLVED: That access to the FLIR system and equipment shall be as follows:

IV. ACCESS TO THE FLIR EQUIPMENT

A. Day to Day Operations

The FLIR is maintained by the FLIR Staff and FLIR Vendors. Only FLIR Staff will be used to monitor incoming FLIR Data.

B. Training

Training by the Chief Privacy Officer is required prior to interaction with the FLIR. All FLIR Staff who are assigned to monitor the FLIR Data will be required to participate in specific training around constitutional rights, protections, and appropriate uses of the FLIR and consequences for violating this Policy.

C. Support and Repairs

City staff and FLIR Vendors that installed the FLIR will have access to the FLIR but may only have access to FLIR Data for the purpose of carrying out their job functions. Any FLIR access by FLIR Vendors requires a background check.

D. Funding Auditing Purposes

Federal, State, or Local funding auditors may have access to only equipment, hardware, and software solely for audit purposes and must abide by the requirements of this Policy.

FURTHER RESOLVED: That access to information and data obtained through the FLIR shall be as follows:

V. ACCESS TO INFORMATION AND DATA OBTAINED THROUGH FLIR

A. Access: Access to the incoming FLIR Data shall be limited exclusively to City employees with a Need To Know. Other than FLIR Staff, any sworn or non-sworn personnel without a

direct role in investigating, auditing, or responding to an incident will not be permitted access to the incoming FLIR Data.

B. **Data Sharing:** The above restriction on access to FLIR Data in Section VI.A does not prohibit the Oakland Police Department from communicating critical information obtained or derived from the FLIR Data, such as a fleeing suspect's location, to outside agencies assisting in the immediate apprehension of a fleeing suspect who is not inside a private residence.

C. **Data Retention:** The FLIR shall not collect (other than real-time), retain, store, or disseminate any data.

FURTHER RESOLVED: That the allowable uses for the FLIR data/system shall be as follows:

VI. ALLOWABLE USES

A. **Uses:** The following situations are the only ones in which use of the FLIR is allowable and may be activated in response to:

Active Shooter	Hot pursuit of suspect
Aircraft accident or fire	Locating vehicles or aircraft in remote areas
Barricaded subject	Missing/abducted person
Firefighting investigation, suppression, or firefighter support	Special Events, as defined by the Oakland Municipal Code, which occur in public places
Facilitating search and rescue efforts over land or water	

B. The FLIR shall not be used to infringe or intrude upon Protected Activity except where all of the following conditions are met:

- 1) There is a Reasonable Suspicion of criminal wrongdoing; and
- 2) FLIR Staff articulates the facts and circumstances surrounding the use and basis for Reasonable Suspicion in a written statement filed with the Chief Privacy Officer no later than 8 hours after use of the FLIR.

FURTHER RESOLVED: That the following internal controls, audits and reporting metrics shall apply to the FLIR data:

VII. INTERNAL CONTROLS, AUDITS AND REPORTING METRICS

A. Chief Privacy Officer

Chief Privacy Officer (CPO) refers to the City Administrator or a senior level employee designated by the City Administrator who is responsible for managing the risks and business impacts of privacy laws and policies. The CPO will determine that procedure manuals, checklists, and other directives used by staff are kept up-to-date and consistent with policies and

procedures related to privacy for the FLIR functions, City measures, or other legislative measures related to privacy issues. The CPO will also oversee any training required to maintain compliance.

B. Internal Controls

Controls should be designed to ensure appropriate access and use of the data related to FLIR activities and to prevent and/or detect unauthorized access or use.

C. Compliance Officer

The Compliance Officer is an employee, designated by the City Administrator, whose responsibilities include ensuring that functions related to the FLIR comply with the Policy, other relevant City policies, and regulatory requirements. In doing so, the Compliance Officer will design operational controls that relate but are not limited to the below areas within the FLIR function. These operational controls shall be presented to the Permanent Privacy Policy Committee annually and upon update.

D. Internal Recordkeeping

FLIR Staff shall keep the enumerated records in this section for a period of no less than two years to support compliance with this Policy and allow for independent third party auditors to readily search and understand the FLIR and FLIR Data. The records shall include, but not be limited to, the below enumerated categories:

1. A written list of who may access the FLIR and FLIR Data and person(s) responsible for authorizing such access.
2. Auditing mechanisms that track and record how the FLIR is accessed and FLIR Data viewed, accessed, shared, analyzed, and deleted. For each such action, the logs shall include timestamps, the person who performed such action, and a justification for it (e.g., specific authorized use, maintenance).
3. **FLIR Usage:** An overview of how the FLIR is used including:
 - a. Listing and number of incident records by incident category
 - b. Timing required to close an incident record
 - c. Actionable events, non-actionable events, and false alarms.
4. **Public Safety Effectiveness:** Summary, general information, and evaluations about whether the FLIR is meeting its stated purpose, to include a review and assessment of:
 - a. Crime statistics for geographic areas where the FLIR was used;
 - b. The occurrences in which information derived from FLIR Data was used for potential criminal investigations;
 - c. Lives saved;
 - d. Incidents in which assistance was provided to persons, property, land and Natural Habitat security.
5. **Information Sharing:** A summary of how information derived from FLIR Data is shared with other non-City entities, to include a review and assessment of:
 - a. The type of information disclosed;
 - b. Justification for disclosure (e.g., warrant, real-time mutual assistance, etc.)

- c. The recipient of the information;
 - d. Dates and times of disclosure; and
 - e. Obligations imposed on the recipient of shared information.
6. **Data Minimization:** A reporting of the incidents, if any, of improper access or disclosure of FLIR Data that do not comply with the Policy, including follow-up procedures, resolutions and consequences.
 7. **Protected Activity Exception:** A reporting of the incidents, if any, of the use of the Protected Activity Exception waiver, as provided in Section VI B, including copies of written certifications, follow-up procedures, resolutions, and consequences.
 8. **Dispute Resolution:** A summary and description of the number and nature of complaints filed by citizens or whistleblowers and the resolution of each, unless prohibited by law or the City's Whistleblower program.
 9. **Requests for Change:** A summary of all requests made to the City Council for approval of the acquisition of additional equipment, software, data, technical capabilities or features, or personnel services, relevant to the functions and uses of the FLIR and the pertinent data, including whether the City approved or rejected the proposal and/or required changes to this Policy before approval.
 10. **Data Retention:** An assessment of compliance with the Data Retention prohibition as stated in the Policy.
 11. **System Access Rights Audit:** The process to provide access and specific permission levels to authorized persons/staff working with the FLIR.
 12. **Public Access:** A summary of the public records requests received, responses, and an evaluation of the appropriateness of records submitted and timeliness of responses.
 13. **Cost:** Total annual cost of the surveillance technology, including ongoing costs, maintenance costs, and personnel costs.

FURTHER RESOLVED: That the following internal control reviews and audits shall apply to the FLIR data/system:

VIII. INTERNAL CONTROL REVIEWS AND AUDITS

A. Internal Control Reviews

The Compliance Officer will perform regular self-assessments (internal control reviews) of the FLIR's Internal Controls and will summarize the findings and remediation plans, if any, and report these to the City Administrator and City Auditor and be made publicly available to the extent the release of such information is not prohibited by law.

B. Audits

The City Auditor will consider the function of the FLIR and the relevant risks to privacy and all civil liberties to determine the scope and frequency of performance audits to be conducted by the City Auditor.

Quarterly and as needed audits of the FLIR will be conducted and made publicly available to the extent the release of such information is not prohibited by law, by the Compliance Officer to

ensure compliance with this Policy. The audit shall include the following information and describe any corrective action taken or needed:

C. Annual Report

The Compliance Officer shall prepare and present an Annual Report that summarizes and includes the results of Internal Recordkeeping, Internal Control Self-Assessments, and Independent Audits to the extent the release of such information is not prohibited by law, and present it to the appropriate Committee of the City Council or to the City Council at a public meeting at a designated timing each year. The City Council should use the Report and the information it is based on to publically reassess whether the FLIR benefits outweigh the fiscal and civil liberties costs.

FURTHER RESOLVED: That the following records management protocols shall apply to the FLIR data/system as follows:

IX. RECORDS MANAGEMENT

A. The FLIR Staff will be the custodian of records; responsible for retention (as noted in Section VII), access to information, and responding to requests for information under California’s Public Records Act.

B. FLIR Staff must comply with all relevant and applicable Data Retention policies and procedures, regulations and laws; and be it

X. PUBLIC INFORMATION REQUESTS

FURTHER RESOLVED: That to the extent the release of such information is not prohibited by law, all protocols and public records, including but not limited to use logs, and audits, shall be available to the public upon request; and be it

XI. SANCTIONS AND ENFORCEMENT REMEDIES

FURTHER RESOLVED: That violations of this Policy shall result in consequences that may include retraining, suspension, termination, and if applicable, criminal fines and penalties, or individual civil liability and attorney’s fees and/or damages as provided by California or Oakland law, depending on the severity of the violation; and be it

XII. SEVERABILITY

FURTHER RESOLVED: That if any section, subsection, sentence, clause or phrase of this Policy is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Policy. The City Council hereby declares that it would have adopted this Policy and each section, subsection, clause or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses or phrases may be declared invalid or unconstitutional.

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