



Surveillance Use Policy

FLIR FirstLook (Gen 2)

San Diego Police Department

PURPOSE

The FLIR FirstLook (Gen 2) Robots are ground-based, remote-controlled robots used to support first responders during critical incidents by providing real-time video imagery and live audio.

USE

The FLIR FirstLook (Gen 2) Robot is authorized to provide remote camera video imagery and audio during incidents involving:

- Barricaded suspects
- Hostage incidents, and
- High-risk tactical operations

The following rules and processes are required prior to each use of a FLIR FirstLook (Gen 2) Robot:

- All requests for FLIR FirstLook (Gen 2) Robot support can be initiated by any personnel who are or plan to be a part of a response to support a specific incident or event with a specific support objective.
- A SWAT or Special Operations Unit supervisor must evaluate the request and approve the operation prior to deployment to support each incident. These SWAT or Special Operations Unit supervisors are specially trained to assess the request and determine if the FLIR FirstLook (Gen 2) Robot operation will comply with the SDPD's authorized uses for this equipment.
- Only authorized members of the SWAT team shall use or be in possession of the FLIR FirstLook (Gen 2) Robot equipment.
- The SWAT unit will ensure that when using the FLIR First Look (Gen 2), all citizen rights will be strictly observed.

Department Procedures associated with the use of the FLIR FirstLook (Gen 2) Robot are:

- DP 3.02 – Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification marks.

DATA COLLECTION

The FLIR FirstLook (Gen 2) Robot can observe and record live video in both the visual spectrum and infrared spectrum, commonly known as "IR," "Night Vision," or "Low-Light" vision, and send that video back to the operator's display screen. The FLIR FirstLook (Gen 2) Robot is also equipped with a microphone and can hear and record live audio and relay that sound back to the operator's controller.

The FLIR FirstLook (Gen 2) Robots are deployed only to specific incidents with a specific objective. The FLIR FirstLook (Gen 2) Robot operator must manually activate the robot's video and audio recording features to capture and record video and audio data per the objectives and goals of the mission.

The FLIR FirstLook (Gen 2) Robot cannot automatically record video, audio, or take photographs without the SWAT Officer activating the feature.



Surveillance Use Policy

FLIR FirstLook (Gen 2)

San Diego Police Department

When a recording is activated, this captured video and audio is regarded as Digital Media Evidence (DME) and is treated as evidence throughout the remainder of the operation until the DME is properly impounded and documented by the SWAT Officers assigned to the operation.

During all operations, the robot operator is trained to make every effort only to capture visual imagery of the law enforcement contact or intended target of observation to protect the privacy of nearby uninvolved citizens and their property.

DATA ACCESS

All DME is retained within the hard drive of the monitor until the - DME is removed from the controller (which also serves as the monitor). Only sworn SWAT personnel may possess the Robot and thus possess collected DME until it is extracted from the hard drive and impounded physically.

Once the DME has been impounded, retention, access, possession, and copying of such evidence are controlled and regulated by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification marks.

Only sworn SDPD Police Officers may become part of the SDPD SWAT Unit. All SDPD SWAT personnel must be approved by the SDPD SWAT Lieutenant and the Commanding Officer of the Special Services Division.

Access to data is granted based on the need-to-know/right-to-know principle, ensuring that only individuals directly involved in the investigation or authorized supervisors can access the data and SD cards.

DATA PROTECTION

All DME is retained within the physical hard drive until the DME is removed from the hard drive and is therefore not accessible to anyone remotely.

All DME is retained using an external data recording device attached to the ground control station. This DME is saved on the hard drive within the external recording device until it is removed by SWAT personnel for impounding and, therefore, not accessible to anyone remotely.

Once DME has been impounded, Data protection becomes the responsibility of the Property Unit or the evidence.com system, and all such evidence is controlled and regulated by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification marks.

DATA RETENTION

Once DME has been impounded physically, evidence retention is the responsibility of the SDPD Property Unit or the evidence.com system, and all such evidence is controlled and regulated by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification marks.

All FLIR FirstLook (Gen 2) Robot DME is impounded in the following way. The DME is extracted from the hard drive and placed onto a portable drive by SWAT personnel. This portable drive is then physically



Surveillance Use Policy

FLIR FirstLook (Gen 2)

San Diego Police Department

impounded in the SDPD Property room and labeled as impounded property. The original SD Card is then purged of data and used again.

The individual who impounded the evidence will be responsible for then wiping the hard drive clean within a reasonable amount of time in order for it to be ready for the next operation.

PUBLIC ACCESS

FLIR FirstLook (Gen 2) Robot-collected DME can only be accessed by SDPD SWAT Unit personnel prior to evidence impound. Once the robot-collected DME is impounded by SWAT Personnel into the SDPD Property Room, access to this DME is controlled and regulated by SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence and Articles Missing Identification marks.

Data may be released to the public via public records request if directly associated with a critical incident defined under California Senate Bill 1421 or in accordance with legal proceedings.

THIRD PARTY DATA SHARING

SWAT Unit personnel do not share data collected by the FLIR FirstLook (Gen 2) robot with third-party vendors. All collected data is impounded physically in the SDPD Property Room in accordance with SDPD Procedure 3.02 – Impound, Release, and Disposal of Property, Evidence, and Articles Missing Identification marks.

TRAINING

All sworn SWAT Officers designated as FLIR FirstLook (Gen 2) operators shall receive appropriate training. Training should include guidance on the use of the FLIR FirstLook (Gen 2), interaction with dispatch and patrol operations, along with a review of relevant policies and procedures, including this policy and any applicable case law. Training should also address local, state, and federal laws related to the use of video recording equipment and privacy.

AUDITING AND OVERSIGHT

The SWAT supervisor or the Special Operations Unit supervisor is assigned the primary oversight and approval of each FLIR FirstLook (Gen 2) Robot deployment and operation. These SWAT supervisors are responsible for ensuring all actions by SWAT Personnel comply with SDPD Department Procedures and the Surveillance Use Policy for each specific FLIR FirstLook (Gen 2) Robot operation.

This technology is also audited by the 481 report which tracks the usage of the whole department's military related equipment. Furthermore, there are times that an incident commander of a SWAT scene is not part of the SWAT unit but may give permission to use the technology in accordance with this use policy.

MAINTENANCE

FLIR FirstLook (Gen 2) Robot equipment is inspected prior to every operation to ensure it is in proper working condition.