BOARD of SUPERVISORS

City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco 94102-4689
Tel. No. (415) 554-5184
Fax No. (415) 554-5163
TDD/TTY No. (415) 554-5227

M E M O R A N D U M

TO: William Scott, Police Chief, Police Department

FROM: Victor Young, Assistant Clerk

DATE: June 14, 2022

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee received the following proposed legislation:

File No. 220606 Administrative Code - Surveillance Technology Policy for Police Department Use of Non-City Entity Surveillance Cameras

Ordinance approving Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras.

If you have comments or reports to be included with the file, please forward them to me at the Board of Supervisors, City Hall, Room 244, 1 Dr. Carlton B. Goodlett Place, San Francisco, CA 94102 or by email at: victor.young@sfgov.org.

cc: Lisa Ortiz, Police Department
Lili Gamero, Police Department
Diana Oliva-Aroche, Police Department
Sgt Stacy Youngblood, Police Department/Commission

City and County of San Francisco
Master Report

City Hall
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94102-4689

File Number: 220606 **File Type:** Ordinance **Status:** 30 Day Rule

Enacted: **Effective:**

Version: 1 **In Control:** Rules Committee

File Name: Administrative Code - Surveillance Technology Policy for Police Department Use of Non-City Entity Surveillance Cameras **Date Introduced:** 05/17/2022

Requester: **Cost:** **Final Action:**

Comment: **Title:** Ordinance approving Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras.

Sponsor: Mayor

History of Legislative File 220606

Ver	Acting Body	Date	Action	Sent To	Due Date	Result
1	President	05/17/2022	ASSIGNED UNDER 30 DAY RULE	Rules Committee	06/16/2022	

[Administrative Code - Surveillance Technology Policy for Police Department Use of Non-City Entity Surveillance Cameras]

Ordinance approving Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras.

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
Additions to Codes are in *single-underline italics Times New Roman font*.
Deletions to Codes are in ~~*strikethrough italics Times New Roman font*~~.
Board amendment additions are in double-underlined Arial font.
Board amendment deletions are in ~~strikethrough Arial font~~.
Asterisks (* * * *) indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. Background.

(a) Administrative Code Chapter 19(B) establishes requirements that City departments must follow before they may use or acquire new Surveillance Technology. Under Administrative Code Section 19B.2(a), a City department must obtain Board of Supervisors approval by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a Board-approved Surveillance Technology ordinance; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology; or (5) entering into an oral or written agreement under which a non-City entity or individual regularly provides the department with data or information acquired through the entity's use of Surveillance Technology.

(b) Under Administrative Code Section 19B.2(b), the Board of Supervisors may approve a Surveillance Technology Policy ordinance under Section 19B.2(a) only if: (1) the

department seeking Board approval first submits to the Committee on Information Technology (COIT) a Surveillance Impact Report for the Surveillance Technology to be acquired or used; (2) based on the Surveillance Impact Report, COIT develops a Surveillance Technology Policy for the Surveillance Technology to be acquired or used; and (3) at a public meeting at which COIT considers the Surveillance Technology Policy, COIT recommends that the Board adopt, adopt with modification, or decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be acquired or used.

(c) Under Administrative Code Section 19B.4, the City policy is that the Board of Supervisors will approve a Surveillance Technology Policy ordinance only if it determines that the benefits that the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

Section 2. Surveillance Technology Policy Ordinance for Police Department Use of Non-City Entity Surveillance Cameras.

(a) Purpose. The Police Department seeks Board of Supervisors authorization under Section 19B.2(a) to use surveillance cameras and surveillance camera networks owned, leased, managed, or operated by non-City entities to: (1) temporarily live monitor activity during exigent circumstances, significant events with public safety concerns, and investigations relating to active misdemeanor and felony violations; (2) gather and review historical video footage for the purposes of conducting a criminal investigation; and (3) gather and review historical video footage for the purposes of an internal investigation regarding officer misconduct.

(b) Surveillance Impact Report. The Police Department submitted to COIT a Surveillance Impact Report for Non-City Entity Surveillance Cameras. A copy of the Police Department Surveillance Impact Report for Non-City Entity Surveillance Cameras is in Board File No. _____, and is incorporated herein by reference.

(c) Public Hearings. Between March 25, 2022 and April 21, 2022, inclusive, COIT and its Privacy and Surveillance Advisory Board (PSAB) conducted four public hearings at which they considered the Surveillance Impact Report referenced in subsection (b) and developed a Surveillance Technology Policy for the Police Department's use of non-City entity surveillance cameras. A copy of the Surveillance Technology Policy for the Police Department's use of the Non-City Entity Surveillance Cameras ("San Francisco Police Department (SFPD) Non-City Entity Surveillance Cameras Policy") is in Board File No. _____, and is incorporated herein by reference.

(d) COIT Recommendation. On April 21, 2022, COIT voted to recommend the SFPD Non-City Entity Surveillance Cameras Policy to the Board of Supervisors for approval.

(e) Findings. The Board of Supervisors hereby finds that the stated benefits of the Police Department's use of non-City entity surveillance cameras outweigh the costs and risks of use of such Surveillance Technology; that the SFPD Non-City Entity Surveillance Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of non-City entity surveillance cameras, as set forth in the SFPD Non-City Entity Surveillance Cameras Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or a protected class.

Section 3. Approval of Policy.

The Board of Supervisors hereby approves the SFPD Non-City Entity Surveillance Cameras Policy.

Section 4. Effective Date. This ordinance shall become effective 30 days after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: /s/ Zachary Porianda
ZACHARY PORIANDA
Deputy City Attorney

n:\govern\as2022\1900636\01602001.docx

FILE NO. 220606

LEGISLATIVE DIGEST

[Administrative Code - Surveillance Technology Policy for Police Department Use of Non-City Entity Surveillance Cameras]

Ordinance approving Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras.

Background Information

Pursuant to Administrative Code Section 19B.2(b), the Police Department seeks Board of Supervisors approval of a surveillance technology policy regarding use of the Non-City Entity Surveillance Cameras ("San Francisco Police Department Non-City Entity Surveillance Cameras Policy"). The proposed Surveillance Technology Policy would authorize the Police Department to use surveillance cameras and surveillance camera networks owned, leased, managed, or operated by non-City entities to: (1) temporarily live monitor activity during exigent circumstances, significant events with public safety concerns, and investigations relating to active misdemeanor and felony violations; (2) gather and review historical video footage for the purposes of conducting a criminal investigation; and (3) gather and review historical video footage for the purposes of an internal investigation regarding officer misconduct.

n:\govern\as2022\1900636\01602069.docx

Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors

From: Carmen Chu, City Administrator
Jillian Johnson, Director, Committee of Information Technology

Date: May 18, 2021

Subject: Legislation introduced to approve Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras

---

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit the Surveillance Technology Policy for the Police Department's use of non-City entity surveillance cameras.

To engage the public in discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held 4 public meetings between March and April to review and approve the policy. All details of these discussions are available at sf.gov/coit.

The following page provides greater detail on the review process for the Surveillance Technology Policy, and COIT's recommended course of action.

If you have questions on the review process please direct them to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Non-City Entity Surveillance Cameras

Department	Authorized Uses
Police Department	1. Temporary live monitoring during an exigency as defined by San Francisco Administrative Code, Section 19B, or Significant Events with public safety concerns, or investigations relating to active misdemeanor and felony violations. Temporary live monitoring will cease, and the connection will be severed within 24 hours after the non-city entity has provided access to SFPD. SFPD shall not record live monitoring however, if misdemeanor or felony violations are observed, nothing in this policy ordinance prohibits SFPD from deferring to authorized use No. 2 or No. 3 of this section. 2. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to a criminal investigation. 3. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to an internal investigation regarding officer misconduct.

Non-City Entity Surveillance Cameras Public Meeting Dates:

Date	Meeting
March 25, 2022	Privacy and Surveillance Advisory Board (PSAB)
March 31, 2022	Privacy and Surveillance Advisory Board (PSAB)
April 7, 2022	Committee on Information Technology (COIT)
April 21, 2022	Committee on Information Technology (COIT)

COIT recommends the following action be taken on the policy:

- Approve the Non-City Entity Cameras Surveillance Technology Policy for the Police Department.

Surveillance Technology Policy

Non-City Entity Surveillance Cameras
San Francisco Police Department (SFPD)

The City and County of San Francisco values the privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of "Non-City Entity" Security Camera System by Department as well as any associated data to which Department is privy, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

Pursuant to the San Francisco Charter, the Police Department is required to preserve the public peace, prevent, and detect crime, and protect the rights of persons and property by enforcing the laws of the United States, the State of California, and the City and County. The Department's mission is to protect life and property, prevent crime and reduce the fear of crime by providing service with understanding, response with compassion, performance with integrity and law enforcement with vision.

The Surveillance Technology Policy ("Policy") defines the way the non-city entity Security Camera System will be used to support department operations.

This Policy applies to all department personnel that use, plan to use, or plan to secure non-city entity security camera systems or data, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

This policy applies to security camera data sharing between SFPD and the following entities:

- Any non-City entity or individual, through consent, subpoena search warrant or other court order, who provides SFPD with data access or information acquired through the entity's or individual's use of surveillance cameras or surveillance camera networks owned, leased, managed and/or operated by the entity or individual. These entities do not have financial agreements with SFPD.

This policy excludes any surveillance cameras that meet both of the following conditions:

- Paid for through a city grant
- Owned by a non-City entity that is under a contractual agreement with the City requiring them to share live feed or historical footage from the camera

SFPD is limited to the following authorized use(s) and requirements listed in this Policy only.

Surveillance Oversight Review Dates
COIT Review: April 21, 2022
Board of Supervisors Review: TBD

Authorized Use(s):

1. Temporary live monitoring during an exigency as defined by San Francisco Administrative Code, Section 19B, or Significant Events with public safety concerns, or investigations relating to active misdemeanor and felony violations. Temporary live monitoring will cease, and the connection will be severed within 24 hours after the non-city entity has provided access to SFPD. SFPD shall not record live monitoring however, if misdemeanor or felony violations are observed, nothing in this policy ordinance prohibits SFPD from deferring to authorized use No. 2 or No. 3 of this section.

2. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to a criminal investigation.

3. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to an internal investigation regarding officer misconduct.

Prohibitions:

- Surveillance camera footage will not on its own identify an individual, confirm racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or information concerning an individual person's sex life or sexual orientation.

- SFPD is prohibited from using biometric identification or facial recognition technology in connection with non-City entity surveillance cameras or associated data.

- SFPD is prohibited from live monitoring inside residential dwellings where homeowners/renters have a reasonable expectation of privacy unless one the following conditions exist: Exigency per SF Admin Code 19b.7; a homeowner/renter/individual with legal authority to do so provides consent; or a warrant is issued. If the conditions exist, SFPD shall adhere to the authorized use and reporting provisions relating to temporary live monitoring.

- SFPD is prohibited from monitoring any certain groups or individuals based, in whole or in part, on race, gender, religion, or sexual orientation. Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action.

- SFPD is prohibited from accessing, requesting, or monitoring any surveillance camera live feed during First Amendment activities for reasons outside of redeployment needs due to crowd sizes or other issues creating public safety hazards. SFPD members are required to comply with SFPD Department General Order (DGO) 8.03 Crowd Control,

DGO 8.10 Guidelines for First Amendment Activities and its annual audit requirements, and the SFPD Event Manual to ensure the safety of those attending planned or spontaneous events.

- SFPD members shall not acquire or use surveillance camera footage in cooperation with or assisting U.S. Immigration and Customs Enforcement or U.S. Customs and Border Protection in any investigation, detention, or arrest procedures, public or clandestine, where in any such instance the purpose is the enforcement of federal immigration laws. SFPD complies with SF Administrative Code Chapters 12H "Immigration Status" and 12I "Civil Immigration Detainers" and SFPD General Order (DGO) 5.15 "Enforcement of Immigration Laws".

BUSINESS JUSTIFICATION

[A description of the product, including vendor and general location of technology]

Categories: Residential, Small Business, Commercial Security Camera Systems.

Subcategories: Indoor, Outdoor

Typical Camera Types [Not vendor specific]:

- Box Camera: A Box Style camera is a standalone camera. The name is derived from the shape of the camera.
- Dome Camera: A dome camera is a combination of camera, lens, and ceiling mount packaged in a discreet dome shape.
- PTZ Camera: A PTZ camera contains mechanical controls that allow the operator to remotely pan, tilt, and zoom the camera.
- Bullet Camera: A bullet camera is a combination of camera, lens, and housing packaged in a bullet-style body.
- IP Camera: An IP camera transmits a digital signal using Internet Protocol over a network
- Wireless IP Camera: Wireless IP security cameras offers ease of installation and eliminates the cost of network cabling when adding this camera to your video surveillance system.
- Day/Night Camera: A Day/night camera is a camera used indoor and outdoor for environments with low light conditions.
- Wide Dynamic Cameras: Wide Dynamic Cameras can balance light-levels on a pixel-by-pixel basis
- Smart/Doorbell Cameras: cameras typically affixed to a or inside of a residence.

Security Cameras supports the Department's mission and provides important operational value in the following ways:

X	Health	Protect safety of visitors and residents of San Francisco.
☐	Environment	

X	Criminal Justice	Review video footage after a crime has occurred; officer and community safety during live monitoring; corroborate witness statements; investigative tool; provide objective video evidence to the DA's office for prosecutorial functions or provide to the public upon request through a formal process, order, or subpoena.
☐	Housing	
X	Other	Effective public-safety interventions to curb crime and improve livability and wellbeing of communities.

In addition, the following benefits are obtained:

Benefit		Description
X	Financial Savings	Non-city entity Security Camera Systems do not require Department operational funding and reduce reliance on first-hand accounts by patrol officers or fixed posts, making deployments more effective and efficient.
X	Time Savings	Non-city entity Security Camera Systems may run 24/7, thus decreasing or eliminating building or patrol officer supervision. Reviewing Third Party data may also decrease demands on investigative units corroborating first-hand accounts of criminal activity.
X	Staff Safety	Non-city entity Security Camera Systems provide situational awareness and increase officer safety, particularly during live video reviews.
X	Service Levels	Non-city entity Security cameras will enhance effectiveness of incident response, criminal investigations, and result in improved level of service. Criminal activity captured through video can help verify the act of the crime and corroborate whether a suspect has been correctly identified and corroborate witness statements to assist with conviction rates.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed, or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Data Collection:

Department shall only collect data required to execute the authorized use case. All surveillance technology data shared with Department by Non-city entity, including PII, shall be classified according to the City's Data Classification Standard.

The surveillance technology collects some or all the following data types:

Data Type(s)	*Format(s)*	*Classification*
Video and Images	MP4, AVI, MPEG	Level 4
Date and Time	MP4 or other format	Level 4
Geolocation data	TXT, CSV, DOCX	Level 4

Notification:

Departments shall rely on the non-city entity vendor to manage public notifications relating to surveillance technology operation at the site of operations through signage in readily viewable public areas in accordance to Section 19.5 of the Administrative Code.

Access:

Prior to accessing or using data, authorized individuals within the Department receive training in system access and operation, and instruction regarding authorized and prohibited uses.

Access to live views and recorded footage is restricted to members who have receive authorization from their officer and charge and have reviewed this policy, connected written directives, and acknowledged on SFPD Power DMS.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed, or shared by the surveillance technology with Level 4 classification:

- Non-sworn members, at the direction of Officer in Charge. The Officer in Charge (OIC) is any member working in a supervisorial capacity over a unit, group, or team. The OIC is not rank specific.
- Q2-Q4, Police Officer
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- Q80-Q82, Captain
- 0488-0490, Commander
- 0400-0402, Deputy Chief
- 0395, Assistant Chief

- 0390, Chief of Police

Live monitoring requests shall be limited to the following roles and job titles upon authorization of a Captain (Q80-Q82) rank:

- Q2-Q4, Police Officer
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q50-Q-52, Sergeant
- Q60-Q62, Lieutenant
- Q80-Q82, Captain

The approving Captain shall use good faith belief or objectively reasonable reliance on information confirming exigency or misdemeanor or felony violations for the basis of approving or denying live monitoring requests. Upon Board of Supervisors approval of this policy ordinance, the Department will determine a mechanism for the ranks Q2 – Q62 to receive Captain rank approval. The Department's Written Directives Unit shall update the "Permission to Search -Form 468" that may be provided to the non-city entity or individual to substantiate the consent for SFPD live monitoring request. The non-city entity or individual retains the right to refuse the request.

Live monitoring viewing rights include the following roles and job titles:

- Q2-Q4, Police Officer
- Q50-Q-52, Sergeant
- Q35-Q37, Assistant Inspector
- Q0380- Q0382, Inspector
- Q60-Q62, Lieutenant
- Q80-Q82, Captain
- 0488-0490, Commander
- 0400-0402, Deputy Chief
- 0395, Assistant Chief
- 0390, Chief of Police

B. Members of the public

Members of the public may request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security:	Department shall secure any PII received from non-city entity or individuals (or shared by non-city entity) against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation, or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification

level(s) as defined by the National Institute of Standards and Technology (NIST) security framework 800-53, or equivalent requirements from other major cybersecurity framework selected by the department.

Departments shall, at minimum, apply the following safeguards to protect surveillance technology information received from non-city entity from unauthorized access and control, including misuse:

- Storage: Any storage of a non-city entity's camera footage must reside in a SFPD specified repository that meets the City's cyber security requirements as well as Department of Justice California Law Enforcement Telecommunications Systems (CLETS) and Criminal Justice Information Services (CJIS) requirements. Video Retrieval Officers may initially store footage provided by a business or individual on a USB or CD. Upon the execution of a city contract with a digital evidence management system vendor, members shall transfer the footage to this system that requires an agency domain and log in. The evidence management system will have a platform that is auditable and can track the source of upload and number of views. This platform will not be accessible to members of the public or anyone without an approved log-in. This platform will meet the requirements of the Office of Contract Administration ("OCA") who promulgates rules and regulations pursuant to Chapter 21 of the San Francisco Administrative Code. The SFPD Contracting Department shall comply with the requirements of Chapter 21 and cooperate to the fullest extent with OCA in the Acquisition of Commodities and Services.
- Audits: SFPD members shall note in the chronological record of investigation ("chron") time/date surveillance footage was requested, approved, or denied by non-city entity, and in the case of live monitoring requests, SFPD members shall note in an incident report and/or the chron the captain's approval, date/time of access, duration of access and outcome of access. Upon implementation of the internal records management system, SFPD members shall note this information in this system. This data will serve as the Department's audit log, which is electronically accessible for on-demand audits
- Reporting: SFPD shall submit an annual surveillance report as outlined in SF Administrative Code Sections 19B.1 and 19B.6. Upon adoption of the non-city entity surveillance camera policy ordinance, SFPD shall submit a quarterly report tracking live monitoring requests to the Police Commission, copying the Clerk of the Board of Supervisors. The reporting requirement shall commence 60 days after the first full quarter following adoption and every quarter thereafter. After the first two years of quarterly reports to the Commission, the Department will thereafter submit a bi-annual report.

Data Sharing:	The Non-city entity is the custodian of its Surveillance Technology data. The non-city entity may share such data with the Department or other entities solely at its discretion. Data is shared by non-city entity with the Department on the following schedule: X Upon Request X As needed Weekly Monthly Other: *A. Internal (City Entity) Data Sharing* Department shares the following data with the recipients: -District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence. -Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with California discovery laws. -The Department of Police Accountability per Section 4.136(j) of the Sn Francisco Charter -Other City agencies impacted by a criminal incident captured by the surveillance camera footage. Data sharing occurs at the following frequency: As needed *B. External (Non-City Entity) Data Sharing* Department shares the following data with the recipients: -Law enforcement partners, as part of a criminal or administrative investigation; Parties to civil litigation, or other third parties, in response to a valid Court Order; Media may receive redacted footage relating to Officer Involved Shooting Townhall meetings or other public safety issues requiring the public's awareness or assistance. To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall: Comply with all applicable laws, rules, and regulations, including but not limited to, to the extent applicable, the California Values Act (Government Code Section 7284 et seq.) which prohibits state and local law enforcement agencies from engaging certain acts related to immigration enforcement.

If determined by Department's general counsel or SFPD's legal division, surveillance camera footage can be disclosed in response to a public information request. Based on legal advice, the department will redact PII as it may be considered investigative/evidentiary material. The Department may use its discretion when releasing investigative/evidentiary material per SFPD DGO 3.16.

Data sharing occurs at the following frequency: As needed

Data Retention:

Department may store and retain PII data shared by the non-city entity only as long as necessary to accomplish a lawful and authorized purpose. Records shall be purged according to the current San Francisco Police Department Records Retention and Destruction Schedule which calls for destruction of intelligence files two years from the last date of entry with the following exceptions:

a) Information may be maintained if it is part of an ongoing investigation or prosecution.

b) All investigative files shall be maintained according to CA Penal Code, Evidence Code, department retention guidelines and according to state and federal law.

c) Records showing violation of these guidelines shall not be destroyed or recollected for the purpose of avoiding disclosure.

The Department's data retention period and justification are as follows:

- Security Camera data shared with Department by Non-city entity will be stored only for the period necessary for investigation or litigation following an incident. As the data is associated with a criminal investigation, the data is retained for a minimum of two years, or as required by State evidence retention laws. Camera footage associated with an officer misconduct or Officer Involved Shooting (OIS) investigation will be maintained in perpetuity.
- Justification: A shorter retention period safeguards PII from inappropriate or unauthorized use by minimizing the period and purposes for which it may be retained. For data affiliated with criminal investigation, two years allows adequate time for the Department and partner departments to access footage to determine whether it constitutes meaningful evidence. If so determined, the SFPD will retain data in a safe environment as required by relevant evidence laws to ensure access for legal discovery.

Data may be stored in the following location:

☒ Local storage (e.g., local server, storage area network (SAN), network-attached storage (NAS), backup tapes, etc.)

☐ Department of Technology Data Center

☐Software as a Service Product

☒Cloud Storage Provider

Data Disposal:	The Police Department does not have a contract or legal agreement with a non-city entity governing non-city entity data use, including but not limited to non-city entity party data use, sharing, signage, retention, and/or disposal. Upon completion of the data retention period, Department shall dispose of data in the following manner: - Delete from local storage - Delete from USB thumb drive or disk if not associated with investigative file
Training:	To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access on behalf of Department must receive training on data security policies and procedures. California Peace Officer Standards and Training (POST) including but not limited to - LD 15 Laws of Arrest - LD 16 Search and Seizure - LD 17 Presentation of Evidence - LD 23 Crimes in Progress - LD 26 Critical Incidents - LD 30 Crime Scenes, Evidence, and Forensics - LD 42 Cultural Diversity/Discrimination - LD 43 Terrorism Awareness - PC 872 (b) Hearsay Testimony SF City & County Employee Portal - Cybersecurity Training SFPD Training - Critical Mindset Coordinated Response Training - DGO 8.10 Guidelines for First Amendment Activities - Video Retrieval Training (two-day) - Crowd Control Training

COMPLIANCE

Department shall oversee and enforce compliance with this Policy according to the respective memorandum of understanding of employees and their respective labor union agreement.

Allegations of 19B Violations: Members of the public may submit written notice of an alleged violation of Chapter 19B to SFPDChief@sfgov.org. If the Department takes corrective measures in response to such an allegation, the Department will post a notice within 30 days that generally describes the corrective measures taken to address such allegation. The Department will comply with allegation and misconduct processes as set forth by the city Charter.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

Sanctions for violations of this Policy include the following:
San Francisco Police Department will conduct an internal investigation though the Chief of Staff/Internal Affairs (IA) Unit or may refer the case to the Department of Police Accountability. The results of the investigation will be reported to the Chief of Police, who will determine the penalty for instances of misconduct. Under San Francisco Charter section A8.343, the Chief may impose discipline of up to a 10-day suspension on allegations brought by the Internal Affairs Division or the Department of Police Accountability. Depending on the severity of the allegation of misconduct, the Chief or the Department of Police Accountability may elect to file charges with the Police Commission for any penalty greater than the 10-day suspension. Any discipline sought must be consistent with principles of just cause and progressive discipline and in accordance with the SFPD Disciplinary Guidelines.

DEFINITIONS

Personally Identifiable Information (PII):	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Significant Events:	These are large or high-profile events in the city where SFPD Special Events Unit and Traffic Company manage street closures, barricades, and crowd management; Special Investigations Division (SID) manages dignitary escorts; or Homeland Security Unit (HSU)/Special Ops is assigned to thwart potential terrorist or criminal attacks. These units may require and request additional deployment efforts

	during these high-profile events based on activity detected during live monitoring which allows for situational awareness and the ability to coordinate resources based on information obtained.
Exigent Circumstances:	See Admin Code Sec. 19B.1

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

QUESTIONS & CONCERNS

Complaints of Officer Misconduct: Members of the public can register complaints about SFPD activities with the Department of Police Accountability (DPA), 1 Van Ness Ave 8th Floor, San Francisco, CA 94103, (415) 241-7711, https://sf.gov/departments/department-police-accountability. DPA, by Charter authority, receives and manages all citizen complaints relating to SFPD. DPA manages, acknowledges, and responds to complaints from members of the public.

Concerns and Inquiries: Department shall acknowledge and respond to concerns in a timely and manner. To do so, the Department has included a 19B Surveillance Technology Policy page on its public website : https://www.sanfranciscopolice.org/your-sfpd/policies/19b-surveillance-technology-policies. This page includes an email address for public inquiries: SFPDChief@sfgov.org. This email is assigned to several staff members in the Chief's Office who will respond to inquiries within 48 hours.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the Chief of Police at SFPDChief@sfgov.org. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the Chief of Police at SFPDChief@sfgov.org

Committee on Information Technology

Office of the City Administrator

To: Members of the Board of Supervisors

From: Carmen Chu, City Administrator
Jillian Johnson, Director, Committee of Information Technology

Date: May 18, 2021

Subject: Legislation introduced to approve Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras

---

In compliance with Section 19B of the City and County of San Francisco's Administrative Code, the City Administrator's Office is pleased to submit the Surveillance Technology Policy for the Police Department's use of non-City entity surveillance cameras.

To engage the public in discussion on the role of government surveillance, the Committee on Information Technology (COIT) and its subcommittee the Privacy and Surveillance Advisory Board (PSAB) held 4 public meetings between March and April to review and approve the policy. All details of these discussions are available at sf.gov/coit.

The following page provides greater detail on the review process for the Surveillance Technology Policy, and COIT's recommended course of action.

If you have questions on the review process please direct them to Jillian Johnson, Director of the Committee on Information Technology (COIT).

Non-City Entity Surveillance Cameras

Department	Authorized Uses
Police Department	1. Temporary live monitoring during an exigency as defined by San Francisco Administrative Code, Section 19B, or Significant Events with public safety concerns, or investigations relating to active misdemeanor and felony violations. Temporary live monitoring will cease, and the connection will be severed within 24 hours after the non-city entity has provided access to SFPD. SFPD shall not record live monitoring however, if misdemeanor or felony violations are observed, nothing in this policy ordinance prohibits SFPD from deferring to authorized use No. 2 or No. 3 of this section. 2. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to a criminal investigation. 3. Requesting, obtaining, and reviewing historical video footage for purposes of gathering evidence relevant to an internal investigation regarding officer misconduct.

Non-City Entity Surveillance Cameras Public Meeting Dates:

Date	Meeting
March 25, 2022	Privacy and Surveillance Advisory Board (PSAB)
March 31, 2022	Privacy and Surveillance Advisory Board (PSAB)
April 7, 2022	Committee on Information Technology (COIT)
April 21, 2022	Committee on Information Technology (COIT)

COIT recommends the following action be taken on the policy:

- Approve the Non-City Entity Cameras Surveillance Technology Policy for the Police Department.

From:	Conine-Nakano, Susanna (MYR)
To:	BOS Legislation, (BOS); PORIANDA, ZACHARY (CAT)
Cc:	Paulino, Tom (MYR); Lee, Ivy (MYR)
Subject:	Mayor -- Ordinance -- Surveillance Technology
Date:	Tuesday, May 17, 2022 4:44:03 PM
Attachments:	01. SFPD Third Party Camera Police Ordinance.DOCX 02. Leg Digest - SFPD ST Policy Ordinance.DOCX

Hello Clerks,

Attached for introduction to the Board of Supervisors is an Ordinance approving Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras.

@PORIANDA, ZACHARY (CAT), can you please reply-all to confirm your approval? Thanks!

Please let me know if you have any questions.

Best,
Susanna

Susanna Conine-Nakano
Office of Mayor London N. Breed
City & County of San Francisco
1 Dr. Carlton B. Goodlett Place, Room 200
San Francisco, CA 94102
415-554-6147

From: Porianda, Zachary (CAT)
To: Conine-Nakano, Susanna (MYR); BOS Legislation, (BOS)
Cc: Paulino, Tom (MYR); Lee, Ivy (MYR)
Subject: RE: Mayor -- Ordinance -- Surveillance Technology
Date: Tuesday, May 17, 2022 4:50:23 PM

I approve.

Thank you,

Zach

Zachary Porianda (he/him/his)
Deputy City Attorney
Office of City Attorney David Chiu
1 Dr. Carlton B. Goodlett Place, Suite 234
San Francisco, CA 94102
phone: (415) 554-4665

https://url.avanan.click/v2/___www.sfcityattorney.org___.YXAzOnNmZHQyOmE6bzo0NDhkN2ZiOTFkNzBlODhlNmUyNDI0YjBhZjhhY2M2ZDo2OjBmMTA6NDM2MWQ3N2M1Yjk0OTAyN2JkNmQ5MGZjZDk0NDc1YWM0MGZhZTc1Nzc2MzhlNmUyNjYxZmFiMTY3YjY1MGUxMzpwOkY

-----Original Message-----
From: Conine-Nakano, Susanna (MYR) <susanna.conine-nakano@sfgov.org>
Sent: Tuesday, May 17, 2022 4:44 PM
To: BOS Legislation, (BOS) <bos.legislation@sfgov.org>; Porianda, Zachary (CAT) <Zachary.Porianda@sfcityatty.org>
Cc: Paulino, Tom (MYR) <tom.paulino@sfgov.org>; Lee, Ivy (MYR) <ivy.lee@sfgov.org>
Subject: Mayor -- Ordinance -- Surveillance Technology

Hello Clerks,

Attached for introduction to the Board of Supervisors is an Ordinance approving Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras.

@PORIANDA, ZACHARY (CAT), can you please reply-all to confirm your approval? Thanks!

Please let me know if you have any questions.

Best,
Susanna

Susanna Conine-Nakano
Office of Mayor London N. Breed
City & County of San Francisco
1 Dr. Carlton B. Goodlett Place, Room 200 San Francisco, CA 94102
415-554-6147

[Administrative Code - Surveillance Technology Policy for Police Department Use of Non-City Entity Surveillance Cameras]

Ordinance approving Surveillance Technology Policy for Police Department use of non-City entity surveillance cameras.

NOTE: **Unchanged Code text and uncodified text** are in plain Arial font.
Additions to Codes are in *single-underline italics Times New Roman font*.
Deletions to Codes are in ~~*strikethrough italics Times New Roman font*~~.
Board amendment additions are in double-underlined Arial font.
Board amendment deletions are in ~~strikethrough Arial font~~.
Asterisks (* * * *) indicate the omission of unchanged Code subsections or parts of tables.

Be it ordained by the People of the City and County of San Francisco:

Section 1. Background.

(a) Administrative Code Chapter 19(B) establishes requirements that City departments must follow before they may use or acquire new Surveillance Technology. Under Administrative Code Section 19B.2(a), a City department must obtain Board of Supervisors approval by ordinance of a Surveillance Technology Policy before: (1) seeking funds for Surveillance Technology; (2) acquiring or borrowing new Surveillance Technology; (3) using new or existing Surveillance Technology for a purpose, in a manner, or in a location not specified in a Board-approved Surveillance Technology ordinance; (4) entering into agreement with a non-City entity to acquire, share, or otherwise use Surveillance Technology; or (5) entering into an oral or written agreement under which a non-City entity or individual regularly provides the department with data or information acquired through the entity's use of Surveillance Technology.

(b) Under Administrative Code Section 19B.2(b), the Board of Supervisors may approve a Surveillance Technology Policy ordinance under Section 19B.2(a) only if: (1) the

department seeking Board approval first submits to the Committee on Information Technology (COIT) a Surveillance Impact Report for the Surveillance Technology to be acquired or used; (2) based on the Surveillance Impact Report, COIT develops a Surveillance Technology Policy for the Surveillance Technology to be acquired or used; and (3) at a public meeting at which COIT considers the Surveillance Technology Policy, COIT recommends that the Board adopt, adopt with modification, or decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be acquired or used.

(c) Under Administrative Code Section 19B.4, the City policy is that the Board of Supervisors will approve a Surveillance Technology Policy ordinance only if it determines that the benefits that the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class.

Section 2. Surveillance Technology Policy Ordinance for Police Department Use of Non-City Entity Surveillance Cameras.

(a) Purpose. The Police Department seeks Board of Supervisors authorization under Section 19B.2(a) to use surveillance cameras and surveillance camera networks owned, leased, managed, or operated by non-City entities to: (1) temporarily live monitor activity during exigent circumstances, significant events with public safety concerns, and investigations relating to active misdemeanor and felony violations; (2) gather and review historical video footage for the purposes of conducting a criminal investigation; and (3) gather and review historical video footage for the purposes of an internal investigation regarding officer misconduct.

(b) Surveillance Impact Report. The Police Department submitted to COIT a Surveillance Impact Report for Non-City Entity Surveillance Cameras. A copy of the Police Department Surveillance Impact Report for Non-City Entity Surveillance Cameras is in Board File No. _____, and is incorporated herein by reference.

(c) Public Hearings. Between March 25, 2022 and April 21, 2022, inclusive, COIT and its Privacy and Surveillance Advisory Board (PSAB) conducted four public hearings at which they considered the Surveillance Impact Report referenced in subsection (b) and developed a Surveillance Technology Policy for the Police Department's use of non-City entity surveillance cameras. A copy of the Surveillance Technology Policy for the Police Department's use of the Non-City Entity Surveillance Cameras ("San Francisco Police Department (SFPD) Non-City Entity Surveillance Cameras Policy") is in Board File No. _____, and is incorporated herein by reference.

(d) COIT Recommendation. On April 21, 2022, COIT voted to recommend the SFPD Non-City Entity Surveillance Cameras Policy to the Board of Supervisors for approval.

(e) Findings. The Board of Supervisors hereby finds that the stated benefits of the Police Department's use of non-City entity surveillance cameras outweigh the costs and risks of use of such Surveillance Technology; that the SFPD Non-City Entity Surveillance Cameras Policy will safeguard civil liberties and civil rights; and that the uses and deployments of non-City entity surveillance cameras, as set forth in the SFPD Non-City Entity Surveillance Cameras Policy, will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or a protected class.

Section 3. Approval of Policy.

The Board of Supervisors hereby approves the SFPD Non-City Entity Surveillance Cameras Policy.

Section 4. Effective Date. This ordinance shall become effective 30 days after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board of Supervisors overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: /s/ Zachary Porianda
ZACHARY PORIANDA
Deputy City Attorney

n:\govern\as2022\1900636\01602001.docx