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: Michael Makstman, Executive Director, Department of Technology

FROM: Victor Young, Assistant Clerk

DATE: May 28, 2026

SUBJECT: LEGISLATION INTRODUCED

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

File No. 260414

Ordinance approving Surveillance Technology Policy governing the use of social media monitoring software for the Fire Department.

If you have comments or reports to be included with the file, please forward them to Victor Young 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.

(attachment)

c. Karen Hong Yee, Department of Technology

City and County of San Francisco
Master Report

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

File Number: 260414 **File Type:** Ordinance **Status:** 30 Day Rule

Enacted: **Effective:**

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

File Name: Administrative Code - Approval of Surveillance Technology Policy for the Fire Department **Date Introduced:** 04/28/2026

Requester: Fire Department **Cost:** **Final Action:**

Comment: **Title:** Ordinance approving Surveillance Technology Policy governing the use of social media monitoring software for the Fire Department.

History of Legislative File 260414

Ver	Acting Body	Date	Action	Sent To	Due Date	Result
1	Clerk of the Board	04/13/2026	RECEIVED FROM DEPARTMENT			
1	President	04/28/2026	ASSIGNED UNDER 30 DAY RULE	Rules Committee	05/28/2026	

[Administrative Code - Approval of Surveillance Technology Policy for the Fire Department]

Ordinance approving Surveillance Technology Policy governing the use of social media monitoring software for the Fire Department.

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) Terms used in this ordinance have the meaning set forth in Administrative Code Chapter 19B ("Chapter 19B").

(b) Chapter 19B 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 (Board) 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.

(c) Under Administrative Code Section 19B.2(b), the Board 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.

(d) Under Administrative Code Section 19B.4, the City policy is that the Board 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 Fire Department Use of Social Media Monitoring Software.

(a) Purpose. The Fire Department seeks Board authorization under Section 19B.2(a) social media monitoring software to: (1) publish the Fire Department's content on social media; (2) communicate with social media users about Fire Department news and share information on services offered through various social media channels; (3) analyze data gathered from social media sources and print media to assess the effectiveness of outreach and optimize messaging to the public to achieve the Fire Department's communication

objectives; and (4) respond to social media users' posts about possible emergencies, fire code violations, and other situations in the purview of the Fire Department.

(b) Surveillance Impact Report. The Fire Department submitted to COIT a Surveillance Impact Report for Social Media Monitoring Software. A copy of the Fire Department Surveillance Impact Report for Non-City Entity Surveillance Cameras is on file with the Clerk of the Board in File No. _____ and incorporated herein by reference.

(c) Public Hearings. On August 24, 2023 and September 21, 2023, inclusive, COIT and its Privacy and Surveillance Advisory Board (PSAB) conducted two public hearings at which they considered the Surveillance Impact Report referenced in subsection (b) and developed a Surveillance Technology Policy for the Fire Department's use of social media monitoring software. A copy of the Surveillance Technology Policy for the Fire Department's use of social media monitoring software ("San Francisco Fire Department (SFFD) Social Media Monitoring Software") is on file with the Clerk of the Board in File No. _____ and incorporated herein by reference.

(d) COIT Recommendation. On September 21, 2023, COIT voted to recommend the SFFD Social Media Monitoring Software Policy to the Board for approval.

(e) Findings. The Board hereby finds that the stated benefits of the Fire Department's use of social media monitoring software outweigh the costs and risks of use of such Surveillance Technology; that the SFFD Social Media Monitoring Software Policy will safeguard civil liberties and civil rights; and that the uses and deployments of social media monitoring software, as set forth in the SFFD Social Media Monitoring Software 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 hereby approves the SFFD Social Media Monitoring Software Policy.

Section 4. Effective Date. This ordinance shall become effective on the 31st day after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within 10 days of receiving it, or the Board overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: _____/s/_____
Sarah Fabian
Deputy City Attorney

4902-3038-5313, v. 1

FILE NO. 260414

LEGISLATIVE DIGEST

[Administrative Code - Surveillance Technology Policy for Fire Department's Use of Social Media Monitoring Software]

Ordinance approving Surveillance Technology Policy for the Fire Department's use of social media monitoring software.

Existing Law

Under Administrative Code Section 19B.2(b), the Fire Department ("Fire") seeks Board of Supervisors approval of a Surveillance Technology Policy regarding the use of social media monitoring software. The proposed Surveillance Technology Policy would authorize Fire to use the technology to : (1) publish the Fire Department's content on social media; (2) communicate with social media users about Fire Department news and share information on services offered through various social media channels; (3) analyze data gathered from social media sources and print media to assess the effectiveness of outreach and optimize messaging to the public to achieve the Fire Department's communication objectives; and (4) respond to social media users' posts about possible emergencies, fire code violations, and other situations in the purview of the Fire Department.

On August 24, 2023, and September 21, 2023, the Committee on Information Technology ("COIT") and its Privacy and Surveillance Advisory Board conducted two public hearings at which they considered the Surveillance Impact Report for Fire's use of social medial monitoring software and developed a Surveillance Technology Policy.

On September 21, 2023, COIT voted to recommend that the Board of Supervisors adopt Fire's Surveillance Technology Policy for the use of social media monitoring software.

Surveillance Technology Policy

Social Media Monitoring Software
Fire Department

The City and County of San Francisco values 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 Social Media Monitoring Software itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

This Surveillance Technology Policy applies to the use of social media monitoring software and technology by the Fire Department.

PURPOSE AND SCOPE

The Surveillance Technology Policy ("Policy") defines the manner in which the surveillance technology will be used to support the missions of the Fire Department, hereby referred to as "the Department", by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all Department personnel that use, plan to use, or plan to secure Social Media Monitoring Software, (hereinafter referred to as "surveillance technology"), including employees, contractors, and volunteers. The only areas of the policy that Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of the surveillance technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– *Publish the Department's content on social media*
– *Communicate with social media users about Department news and share information on services offered through various social media channels*
– *Analyze data gathered from social media sources and print media to assess the effectiveness of outreach and optimize messaging to the public to achieve the Department's communication objectives*
– *Respond to social media users' posts about possible emergencies, fire code violations, and other situations in the purview of the Fire Department.*

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Surveillance Oversight Review Dates
PSAB Review: 8/24/2023
COIT Review: TBD
Board of Supervisors Approval: TBD

Department may use information collected from technology only for legally authorized purposes and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data.

BUSINESS JUSTIFICATION

Reason for Technology Use

The surveillance technology supports the Department's missions by allowing the Department to communicate with members of the public, including City residents, workers, and visitors, about city services on platforms which the public already uses. By employing social media monitoring technology to aggregate data and communicate across social media platforms, the technology allows Department to quickly communicate a consistent message across platforms, respond to constituent concerns in a timely manner, use post engagement information to strategize on the most effective way to reach specific audiences, and collect vital information on the public's concerns and need for government services.

Description of Technology

A social media monitoring technology is a technology from which a department can review all their social media accounts in one place, search all accounts and public content at once by typing in key words through a dashboard interface, schedule posts in advance on social media platforms and analyze the engagement with those posts. While the specific functions of each tool may vary, the technology often allows conversations to be labeled for later reference and can save content posted to social media platforms by other users. Search terms can be saved so that they can be repeated in the future, supporting customized monitoring across social media platforms.

Examples of social media monitoring technologies potentially used by the Department include:

- AgoraPulse
- Archive Social
- Buffer
- Critical Mention
- Falcon/ Brandwatch
- Hootsuite
- Later.com
- Meltwater
- Meta Business Manager and Meta Business Suite
- Sendible
- Sprout Social
- Tweetdeck

Resident Benefits

The social media monitoring software allows the Department to communicate with the public about services and programs offered by the Department, improving the accessibility of these services.

The distinct services provided by the Department, made more accessible through the surveillance technology, include the following benefits:

Benefit	Description
Education	The technology allows the department to inform the public about city and county – provided programs, services, facilities and or benefits using social media services that the public already uses.
Community Development	The technology allows the department to communicate with San Francisco residents about city and county-provided programs, services, facilities, and/or benefits. It also allows the department to gather community feedback via social media engagement by residents with the department's social media accounts.
Public Safety	The technology allows the department to quickly respond to questions/problems raised by residents in multiple public forums.

Department Benefits

The surveillance technology will benefit the department in the following ways:

Benefit	Description
Financial Savings	The social media monitoring software presents financial benefits by reducing the number of staff assigned to the Department's social media work.
Time Savings	The social monitoring software helps the Department save time by allowing social media management with fewer staff members than would be needed if the software was not being used.

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.

Specifications: The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

Data Collection:

The Department shall only collect data required to execute the authorized use cases. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

The surveillance technology collects some or all of the following data type(s):

Data Type(s)	*Format(s)*	*Classification*
Social media handles, profiles, and posts (which can include name, date of birth, age, location, marital and employment status)	HTML, JPG, PNG, GIF, MOV, MP3, MP4.	Level 1-3
Biometric information, insofar that it is captured by the social media platform, e.g., Facebook and Instagram.	HTML, JPG, PNG, GIF, MOV, MP3, MP4.	Level 3

Access:

All parties requesting access must adhere to the following rules and processes:

- **Training:** The Department will train their staff with access to the social media monitoring technology on how to properly use the technology, which will include information from the manufacturer on how to use their technology as well as information about this surveillance technology policy and the authorized use cases.
- **Documented Guidelines:** The Department will create a written social media guideline document for the reference of their employees regarding appropriate and prohibited uses, information about the data lifecycle for the technology, and a discussion of how to avoid any applicable civil liberties concerns.

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:

- H039 - Fire Captain - Public Information Officer (1)

B. Members of the public

Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed.

Members of the public may also 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.

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 must receive training on data security policies and procedures.

Department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and confirm that they understand all authorized and prohibited uses dictated by this policy. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

More specifically, Department training will include:

All department staff with authorized access to the technology will receive training on how to use the social media monitoring technology, including information on data security best practices.

Data Security: 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. Access to the surveillance technology will be restricted to only necessary department personnel and will be monitored by the department for misuse, either by city and county staff or by external malicious actors.

Department shall ensure compliance with these security standards through the following:

Only necessary department personnel will have access to the social media monitoring technology login information. Only software with encryption will be used. No sensitive information or Personally Identifiable Information ("PII") should be solicited through the social media monitoring technology by the department.

Data Storage: The Department included in this policy may store information in one or more of the following ways: Cloud Storage Provider, DT Data Center, Local Storage, and/or Software as a Service.

Data Sharing: The Department will endeavor to ensure that other agencies or departments that may receive data collected by the surveillance technology will act in conformity with this Policy.

For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. *(See Data Security)*

Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded from entities that do not have authorized access under this policy.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their legal obligations.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- Confirm the purpose of the data sharing aligns with the department's mission.
- Consider alternative methods other than sharing data that can accomplish the same purpose.
- Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.

- Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Department does not share data either internally with city and county departments or externally with entities outside of the City and County of San Francisco.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose. Department data retention standards should align with how the department prepares its financial records and should be consistent with any relevant Federal Emergency Management Agency (FEMA) or California Office of Emergency Services (Cal OES) sections.

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

Retention Period	Retention Justification
A report summarizing the social media activity via the social media monitoring software's analysis is circulated to department leadership, who can view the document for a maximum of 30 days.	This is a monthly report and only needs to be retained until the next report is issued.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed.

Data Disposal:	Upon completion of the data retention period, Department shall dispose of data in the following manner: Any file that is downloaded from the social media monitoring software must be deleted in no longer than the maximum time allowed by the retention period. A department must check for these files on a regular basis and this process must be a part of the training that department employees authorized to use the surveillance technology are given. All materials are deleted after the requisite retention period.

COMPLIANCE

The Department are responsible for ensuring compliance with this policy within their own Department, and across third-party entities acting on their behalf.

Department Compliance

Department shall oversee and enforce compliance with this Policy using the following methods:

The department will conduct an annual review of technology policy and best practices to ensure compliance and will require training for all authorized personnel.

Interdepartmental, Intergovernmental & Non-Governmental Entity Compliance

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall not share data with other entities.

Oversight Personnel

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third parties.

1070 - IS Project Director / 0941 - Chief Information Officer

Sanctions for Violations

Sanctions for violations of this Policy include the following:

- First offense: violator shall be verbally notified by Fire Department management of nature of violation.
- Second offense: violator shall be notified in writing of second offense and privileges to run queries in Critical Mention will be suspended for 30 days.
- Third offense: disciplinary action may be taken depending upon the severity of second/third offences.

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.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

DEFINITIONS

Personally-Identifiable Information:	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.
Raw Data:	Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

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

Public Inquiries

Questions or complaints can be submitted through the Department website: https://sf-fire.org/report-fire-safety-concerns-complaints

Department shall acknowledge and respond to complaints and concerns in a timely and organized response, and in the following manner:

All comments received through the Department website are actively monitored and responded to within two weeks or less.

Inquiries from City and County of San Francisco Employees

All questions regarding this policy should be directed to the employee's supervisor or director. Similarly, questions about other applicable laws governing the use of surveillance technology or the issues related to privacy should be directed to the employee's supervisor or director.

Surveillance Impact Report

Social Media Monitoring Software
Fire Department

As required by San Francisco Administrative Code, Section 19B, departments must submit a Surveillance Impact Report for each surveillance technology to the Committee on Information Technology ("COIT") and the Board of Supervisors.

The Surveillance Impact Report details the benefits, costs, and potential impacts associated with the Department's use of Social Media Monitoring Software, (hereinafter referred to as "surveillance technology").

DESCRIPTION OF THE TECHNOLOGY

The Department use the surveillance technology to communicate with members of the public about departmental programs, services, and news.

The Department shall use the surveillance technology only for the following authorized purposes:

Authorized Use(s):

– *Publish the Department's content on social media.*
– *Communicate with social media users about Department news and share information on services offered through various social media channels.*
– *Analyze data gathered from social media sources to optimize outreach to general public and achieve Department's communication objectives.*
– *Respond to social media users' posts about possible emergencies, fire code violations, and other situations in the purview of the Fire Department.*

The technology may be deployed in the following locations, based on use case:

This technology is a software which is used by city and county staff on city-issued devices to communicate with members of the public through the Internet.

Technology Details

This is a product description of the technology:

A social media monitoring technology is a technology from which a department can review all their social media accounts in one place, search all accounts and public content at once by typing in key words through a dashboard interface, schedule posts in advance on social media platforms and analyze the engagement with those posts. While the specific functions of each tool may vary, the technology often allows conversations to be labeled for later reference and can save content posted

to social media platforms by other users. Search terms can be saved so that they can be repeated in the future, supporting customized monitoring across social media platforms.

Examples of social media monitoring technologies potentially used by the Department include:

- AgoraPulse
- Archive Social
- Buffer
- Critical Mention
- Falcon/ Brandwatch
- Hootsuite
- Later.com
- Meltwater
- Meta Business Manager and Meta Business Suite
- Sendible
- Sprout Social
- Tweetdeck

This is a description of how the technology works:

To function, the surveillance technology is a social network manager that allows users to create custom views of all connected social networks. The technology can be used to post to multiple social media accounts, manage social media messaging, and coordinate the organization's social media marketing. The platform aggregates social media feeds so that content and trends can be viewed holistically.

Third-Party Vendor Access to Data

All data collected or processed by the surveillance technology will be handled or stored by an outside provider or third-party vendor on an ongoing basis. Specifically, data will be handled by the third-party company which provides the social media monitoring software to ensure the Department may continue to use the technology.

IMPACT ASSESSMENT

The impact assessment addresses the conditions for surveillance technology approval, as outlined by the Standards of Approval in San Francisco Administrative Code, Section 19B:

1. The benefits of the surveillance technology outweigh the costs.
2. The Department's Policy safeguards civil liberties and civil rights.
3. The uses and deployments of the surveillance technology are not based upon discriminatory or viewpoint-based factors and do not have a disparate impact on any community or Protected Class.

The Department's use of the surveillance technology is intended to support and benefit the residents of San Francisco while minimizing and mitigating all costs and potential civil rights and liberties impacts of residents.

A. Benefits

The Department's use of the surveillance technology has the following benefits for the residents of the City and County of San Francisco:

Benefit	Description
Education	The technology allows the department to inform the public about city and county – provided programs, services, facilities and or benefits using social media services that the public already uses.
Community Development	The technology allows the department to communicate with San Francisco residents about city and county-provided programs, services, facilities, and/or benefits. It also allows the department to gather community feedback via social media engagement by residents with the department's social media accounts.
Public Safety	The technology allows the department to quickly respond to questions/problems raised by residents in multiple public forums.

B. Civil Rights Impacts and Safeguards

The Department has considered the potential impacts and has identified the technical, administrative, and physical protections as mitigating measures:

- Discrimination: Although the information on social media websites is by default public and exists in the public sphere, there is documented evidence that shows that federal entities in the United States have used social media monitoring technologies to collect information about individuals or groups as part of investigations, sometimes without sufficient justification or oversight. These investigations can target certain ethnic groups or nationalities. If the technology is used in this way, it could lead to discriminatory outcomes.
- Loss of Liberty & Loss of Trust: Governments could misuse social media monitoring tools to identify and target individuals or groups expressing dissenting opinions or criticizing government policies. This could lead to unwarranted surveillance and a chilling effect on freedom of speech and expression. Additionally, this can erode trust in government.

The administrative safeguards are that the Department will make sure that only authorized personnel have access to the surveillance technology. Access will be revoked if someone moves to a job without approved access.

The technical safeguards are that the surveillance technology access will be password protected, with passwords that comply with cybersecurity best practices. Departments will only use platforms that pass internal cybersecurity approvals. Authorized personnel will only access the technology from applications and devices approved for use by city and county cybersecurity standards.

C. Fiscal Analysis of Costs and Benefits

The Department's use of the surveillance technology yields the following business and operations benefits:

Benefit	Description
Financial Savings	The social media monitoring software presents financial benefits by reducing the number of staff who need to work on the Department's social media work
Time Savings	The social monitoring software helps the Department save time by allowing social media management with fewer staff members than would be needed if the software was not being used.

The fiscal cost, such as initial purchase, personnel and other ongoing costs, include:

Number of Budgeted FTE (new & existing) & Classification	H039 - Fire Captain - Public Information Officer (1)	
	Annual Cost	***One-Time Cost***
Total Salary & Fringe	$6,995	0
Software	3,450.00	0
Hardware/Equipment	0	0
Professional Services	0	0
Training	0	0
Other	0	0
Total Cost	$3450.00	None

The Department funds its use and maintenance of the surveillance technology through the General Fund.

COMPARISON TO OTHER JURISDICTIONS

The surveillance technology is currently utilized by other governmental entities for similar purposes. Other government entities have used the surveillance technology in the following way:

> Social media monitoring technology has been used by many local, state and national government entities in the United States and internationally to engage their constituents and communicate effectively with them using social media platforms for engagement. Platforms such as Hootsuite and Meltwater report[1] that government entities and other organizations in the public sector use their services, such as Barcelona City Council, the government of British Colombia, the West Midlands Police Department, the city of Boston and the London Metropolitan Police Department.
>
> While many government entities use these platforms to communicate quickly and effectively with constituents, social media monitoring technologies have also been used by law enforcement entities, such as the Department of Homeland Security, the Federal Bureau of Investigation, and the State Department, to gather information about social media users for investigations[2]. These kinds of investigations can particularly impact immigrants to a country where they have not yet acquired citizenship[3].

The effectiveness of the surveillance technology while used by government entities is determined to be the following:

> Social media monitoring technologies allow for government entities to better understand social media trends, how people are communicating online about certain topics, and how they are interacting with certain accounts across the social media ecosystem. A social media monitoring technology assists its users with those goals.
>
> Social media monitoring tools also allow government entities to quickly share important announcements, news updates, and emergency information with their communities, across platforms. This real-time communication can be particularly effective in situations where

[1] *See Hootsuite at https://www.hootsuite.com/industries/government and Meltwater at https://www.meltwater.com/en/industry/public-sector*).
[2] *See Brennan Center for Justice report at https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government#:~:text=The%20Department%20of%20Homeland%20Security,to%20screening%20travelers%20and%20immigrants*.).
[3] *See ACLU report at https://www.aclu.org/news/national-security/is-the-government-tracking-your-social-media-activity*

immediate action or awareness is required. Moreover, the tools offer a more time-efficient way of reaching a large audience given one post can be placed across various social media platforms, reducing the time it takes to communicate with the public.

The adverse effects of the surveillance technology while it has been used by other government entities are:

Effect	Description
Civil Rights and/or Civil Liberties Abuse	Government entities can use the tools included in social media monitoring technologies to surveil communications and investigate people in spaces of communication. These tools make it easier to search for key words and to monitor trends in speech, which could make people not want to speak freely or organize protests that are lawful.

SAN FRANCISCO FIRE DEPARTMENT

TO: **Angela Calvillo, Clerk of the Board of Supervisors**

FROM: **Mark Corso, Finance, San Francisco Fire Department**

DATE: **April 13, 2026**

SUBJECT: **Ordinance Approving Surveillance Technology Policy for the Fire Department**

Dear Ms. Calvillo:

Attached please find electronic copies of the Fire Department's proposed ordinance for the Board of Supervisors to approve, which is an ordinance approving a Surveillance Technology Policy for Social Media Monitoring software for the Fire Department. This policy is a requirement under Administrative Code section 19(B) pertaining to the acquisition of surveillance technology.

Attached please find the following:

X Proposed ordinance
X Proposed legislative digest for ordinance
X COIT-approved Surveillance Technology Policy for this item
X COIT-approved Surveillance Impact Report for this item

Please let me know if there is anything else needed. Thank you.

Special Timeline Requirements: N/A

Departmental representative to receive a copy of the adopted ordinance:

Name: Mark Corso Phone: 558-3417

Interoffice Mail Address: 698 Second Street, San Francisco 94107

Certified copy required Yes ☐ No ☒

From:	Corso, Mark (FIR)
To:	BOS Legislation, (BOS)
Cc:	FABIAN, SARAH (CAT)
Subject:	FIR Proposed Ordinance - Surveillance Technology Policy
Date:	Monday, April 13, 2026 12:22:31 PM
Attachments:	Clerk Memo Social Media monitoring FIR.pdf FIR Social Media Monitoring Software SIR - PSAB Review.pdf FIR Social Media Monitoring Software STP - PSAB Review.pdf Ordinance - final.docx SFFD Social Media Monitoring Legislative Digest.docx

---

Good afternoon. Apologies for trying to sneak this in under the wire, but I am attaching a Fire Department request for ordinance approval by the Board. This ordinance pertains to approval of a Surveillance Technology Policy for the Fire Department pertaining to social media monitoring software.

I have attached our cover letter, the ordinance, the legislative digest, and supporting documentation from COIT approval.

We have worked closely with our DCA on this, cc'd here. Please let either of us know if there are any questions or further information needed. Thank you.

Mark Corso (he, him, his)
Deputy Director
Finance & Planning Division
San Francisco Fire Department
Tel (415) 558-3417

From: Fabian, Sarah (CAT)
To: BOS Legislation, (BOS); Corso, Mark (FIR); BOS Legislation, (BOS)
Subject: RE: FIR Proposed Ordinance - Surveillance Technology Policy
Date: Monday, April 13, 2026 1:47:16 PM
Attachments: image002.png
image004.png

This is approved. You may use my signature.

Thanks,

Sarah

Sarah L. Fabian *(she/her)*
Deputy City Attorney
Office of City Attorney David Chiu
(415) 554-4679 Direct (email preferred)
www.sfcityattorney.org

NOTE ** I am working remotely intermittently and email is the best way to reach me.

From: BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Sent: Monday, April 13, 2026 1:28 PM
To: Corso, Mark (FIR) <mark.corso@sfgov.org>; BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Cc: Fabian, Sarah (CAT) <Sarah.Fabian@sfcityatty.org>
Subject: RE: FIR Proposed Ordinance - Surveillance Technology Policy

Hi Mark,

We are seeking the approval from Deputy City Attorney Sarah Fabian for use of her electronic signature and approval as to form for the proposed Ordinance, by reply to this email.

Since this was received today at 12:22 p.m., this is slated to be introduced the week of April 28, 2026. Please let us know if you have any questions. Thank you.

Best regards,
Jocelyn Wong
Legislative Clerk

San Francisco Board of Supervisors
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, CA 94102
T: 415.554.7702 | F: 415.554.5163
jocelyn.wong@sfgov.org | www.sfbos.org


Click here to complete a Board of Supervisors Customer Service Satisfaction form

The Legislative Research Center provides 24-hour access to Board of Supervisors legislation, and archived matters since August 1998.

From: Corso, Mark (FIR) <mark.corso@sfgov.org>
Sent: Monday, April 13, 2026 12:22 PM
To: BOS Legislation, (BOS) <bos.legislation@sfgov.org>
Cc: FABIAN, SARAH (CAT) <Sarah.Fabian@sfcityatty.org>
Subject: FIR Proposed Ordinance - Surveillance Technology Policy

Good afternoon. Apologies for trying to sneak this in under the wire, but I am attaching a Fire Department request for ordinance approval by the Board. This ordinance pertains to approval of a Surveillance Technology Policy for the Fire Department pertaining to social media monitoring software.

I have attached our cover letter, the ordinance, the legislative digest, and supporting documentation from COIT approval.

We have worked closely with our DCA on this, cc'd here. Please let either of us know if there are any questions or further information needed. Thank you.

Mark Corso (he, him, his)
Deputy Director
Finance & Planning Division
San Francisco Fire Department
Tel (415) 558-3417

[Administrative Code - Approval of Surveillance Technology Policy for the Fire Department]

Ordinance approving Surveillance Technology Policy governing the use of social media monitoring software for the Fire Department.

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) Terms used in this ordinance have the meaning set forth in Administrative Code Chapter 19B ("Chapter 19B").

(b) Chapter 19B 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 (Board) 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.

(c) Under Administrative Code Section 19B.2(b), the Board 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.

(d) Under Administrative Code Section 19B.4, the City policy is that the Board 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 Fire Department Use of Social Media Monitoring Software.

(a) Purpose. The Fire Department seeks Board authorization under Section 19B.2(a) social media monitoring software to: (1) publish the Fire Department's content on social media; (2) communicate with social media users about Fire Department news and share information on services offered through various social media channels; (3) analyze data gathered from social media sources and print media to assess the effectiveness of outreach

and optimize messaging to the public to achieve the Fire Department's communication objectives; and (4) respond to social media users' posts about possible emergencies, fire code violations, and other situations in the purview of the Fire Department.

(b) Surveillance Impact Report. The Fire Department submitted to COIT a Surveillance Impact Report for Social Media Monitoring Software. A copy of the Fire Department Surveillance Impact Report for Non-City Entity Surveillance Cameras is on file with the Clerk of the Board in File No. _____ and incorporated herein by reference.

(c) Public Hearings. On August 24, 2023 and September 21, 2023, inclusive, COIT and its Privacy and Surveillance Advisory Board (PSAB) conducted two public hearings at which they considered the Surveillance Impact Report referenced in subsection (b) and developed a Surveillance Technology Policy for the Fire Department's use of social media monitoring software. A copy of the Surveillance Technology Policy for the Fire Department's use of social media monitoring software ("San Francisco Fire Department (SFFD) Social Media Monitoring Software") is on file with the Clerk of the Board in File No. _____ and incorporated herein by reference.

(d) COIT Recommendation. On September 21, 2023, COIT voted to recommend the SFFD Social Media Monitoring Software Policy to the Board for approval.

(e) Findings. The Board hereby finds that the stated benefits of the Fire Department's use of social media monitoring software outweigh the costs and risks of use of such Surveillance Technology; that the SFFD Social Media Monitoring Software Policy will safeguard civil liberties and civil rights; and that the uses and deployments of social media monitoring software, as set forth in the SFFD Social Media Monitoring Software 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 hereby approves the SFFD Social Media Monitoring Software Policy.

Section 4. Effective Date. This ordinance shall become effective on the 31st day after enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the ordinance unsigned or does not sign the ordinance within 10 days of receiving it, or the Board overrides the Mayor's veto of the ordinance.

APPROVED AS TO FORM:
DAVID CHIU, City Attorney

By: _____/s/_____
Sarah Fabian
Deputy City Attorney

4902-3038-5313, v. 1