

File No. 190110

Committee Item No. 1

Board Item No. _____

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee

Date May 6, 2019

Board of Supervisors Meeting

Date _____

Cmte Board

- | | | |
|-------------------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | Motion |
| <input type="checkbox"/> | <input type="checkbox"/> | Resolution |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Ordinance |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Legislative Digest |
| <input type="checkbox"/> | <input type="checkbox"/> | Budget and Legislative Analyst Report |
| <input type="checkbox"/> | <input type="checkbox"/> | Youth Commission Report |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Introduction Form |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Department/Agency Cover Letter and/or Report |
| <input type="checkbox"/> | <input type="checkbox"/> | Memorandum of Understanding (MOU) |
| <input type="checkbox"/> | <input type="checkbox"/> | Grant Information Form |
| <input type="checkbox"/> | <input type="checkbox"/> | Grant Budget |
| <input type="checkbox"/> | <input type="checkbox"/> | Subcontract Budget |
| <input type="checkbox"/> | <input type="checkbox"/> | Contract/Agreement |
| <input type="checkbox"/> | <input type="checkbox"/> | Form 126 - Ethics Commission |
| <input type="checkbox"/> | <input type="checkbox"/> | Award Letter |
| <input type="checkbox"/> | <input type="checkbox"/> | Application |
| <input type="checkbox"/> | <input type="checkbox"/> | Form 700 |
| <input type="checkbox"/> | <input type="checkbox"/> | Vacancy Notice |
| <input type="checkbox"/> | <input type="checkbox"/> | Information Sheet |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Public Correspondence |

OTHER (Use back side if additional space is needed)

<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____
<input type="checkbox"/>	<input type="checkbox"/>	_____

Completed by: Victor Young

Date May 1, 2019

Completed by: _____

Date _____

[Administrative Code - Acquisition of Surveillance Technology]

1
2 Ordinance amending the Administrative Code to require that City departments
3 acquiring Surveillance Technology, or entering into agreements to receive information
4 from non-City owned Surveillance Technology, submit a Board of Supervisors
5 approved Surveillance Technology Policy Ordinance, based on a policy developed by
6 the Committee on Information Technology (COIT), and a Surveillance Impact Report to
7 the Board in connection with any request to appropriate funds for the purchase of such
8 technology or to accept and expend grant funds for such purpose, or otherwise to
9 procure Surveillance Technology equipment or services; require each City department
10 that owns and operates existing surveillance technology equipment or services to
11 submit to the Board a proposed Surveillance Technology Policy Ordinance governing
12 the use of the surveillance technology; and requiring the Controller, as City Services
13 Auditor, to audit annually the use of surveillance technology equipment or services
14 and the conformity of such use with an approved Surveillance Technology Policy
15 Ordinance and provide an audit report to the Board of Supervisors.

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

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

24 Section 1. General Findings.
25

1 (a) It is essential to have an informed public debate as early as possible about
2 decisions related to surveillance technology.

3 (b) Whenever possible, decisions relating to surveillance technology should occur with
4 strong consideration given to the impact such technologies may have on civil rights and civil
5 liberties, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments
6 to the United States Constitution as well as Sections 1, 2, and 13 of Article I of the California
7 Constitution.

8 (c) While surveillance technology may threaten the privacy of all of us, surveillance
9 efforts have historically been used to intimidate and oppress certain communities and groups
10 more than others, including those that are defined by a common race, ethnicity, religion,
11 national origin, income level, sexual orientation, or political perspective.

12 (d) The propensity for facial recognition technology to endanger civil rights and civil
13 liberties substantially outweighs its purported benefits, and the technology will exacerbate
14 racial injustice and threaten our ability to live free of continuous government monitoring.

15 (e) Whenever possible, decisions regarding if and how surveillance technologies
16 should be funded, acquired, or used, and whether data from such technologies should be
17 shared, should be made only after meaningful public input has been solicited and given
18 significant weight.

19 (f) Legally enforceable safeguards, including robust transparency, oversight, and
20 accountability measures, must be in place to protect civil rights and civil liberties before any
21 surveillance technology is deployed; and

22 (g) If a surveillance technology is approved, data reporting measures must be adopted
23 that empower the Board of Supervisors and the public to verify that mandated civil rights and
24 civil liberties safeguards have been strictly adhered to.

25 ///

1 Section 2. The Administrative Code is amended by adding Chapter 19B, consisting of
2 Sections 19B.1-19B.8, to read as follows:

3
4 **CHAPTER 19B: ACQUISITION OF SURVEILLANCE TECHNOLOGY**

5
6 **SEC. 19B.1. DEFINITIONS.**

7 "Annual Surveillance Report" means a written report that includes all of the following:

8 (1) A general description of how the Surveillance Technology was used;

9 (2) A general description of whether and how often data acquired through the use of the
10 Surveillance Technology item was shared with outside entities, the name of any recipient outside entity,
11 the type(s) of data disclosed, under what legal standard(s) the data was disclosed, and the justification
12 for the disclosure(s);

13 (3) A summary of complaints or concerns from the public about the Surveillance
14 Technology item;

15 (4) The aggregate results of any internal audits required by the Surveillance Technology
16 Policy, any general, aggregate information about violations of the Surveillance Technology Policy, and
17 a general description of any actions taken in response;

18 (5) Information, including crime statistics, which help the Board of Supervisors assess
19 whether the Surveillance Technology has been effective at achieving its identified purposes;

20 (6) Aggregate statistics and information about any Surveillance Technology related to
21 Public Records Act requests;

22 (7) Total annual costs for the Surveillance Technology, including personnel and other
23 ongoing costs, and what source of funding will fund the Surveillance Technology in the coming year;

24 (8) Any requested modifications to the Surveillance Technology Policy and a detailed
25 basis for the request;

1 (9) Where applicable, a general breakdown of what physical objects the Surveillance
2 Technology hardware was installed upon, using general descriptive terms; for Surveillance Technology
3 software, a general breakdown of what data sources the Surveillance Technology was applied to; and

4 (10) A description of products and services acquired or used in the preceding
5 year that are not already included in the Surveillance Technology Policy, including
6 manufacturer and model numbers, and the identity of any entity or individual that provides to
7 the Department services or equipment essential to the functioning or effectiveness of the
8 Surveillance Technology; and

9 (11) A summary of all requests for Board of Supervisors' approval for a Surveillance
10 Technology Policy ordinance.

11 An Annual Surveillance Report shall not contain the specific records that a Surveillance
12 Technology item collects, stores, exchanges, or analyzes and/or information protected, restricted,
13 and/or sealed pursuant to State and/or federal laws, including information exempt from disclosure
14 under the California Public Records Act.

15 "City" means the City and County of San Francisco.

16 "City Department" or "Department" means any City official, department, board, commission,
17 or other entity in the City except that it shall not mean the District Attorney or Sheriff when performing
18 their investigative or prosecutorial functions, provided that:

19 (1) The District Attorney or Sheriff certifies in writing to the Controller that acquisition
20 of a specific Surveillance Technology is necessary to perform an investigative or prosecutorial
21 function. The certification shall identify the Surveillance Technology acquired or to be acquired
22 and shall be a public record; and

23 (2) The District Attorney or Sheriff provides in writing to the Controller either an
24 explanation of how compliance with this Chapter 19B will obstruct their investigative or prosecutorial
25 function or a declaration that the explanation itself will obstruct either function.

1 For purposes of subsection 19B.2(d) only, "City Department" and "Department" shall
2 not include federally-regulated facilities at the Airport or Port.

3 "COIT" means the Committee on Information Technology.

4 "Exigent circumstances" means an emergency involving imminent danger of death or serious
5 physical injury to any person that requires the immediate use of Surveillance Technology or the
6 information it provides.

7 "Face recognition technology" means an automated or semi-automated process that assists in
8 identifying or verifying an individual based on an individual's face.

9 "Surveillance Impact Report" means a written report that includes at a minimum the following:

10 (1) Information describing the Surveillance Technology and how it works, including
11 product descriptions from manufacturers;

12 (2) Information on the proposed purpose(s) for the Surveillance Technology;

13 (3) If applicable, the general location(s) it may be deployed and crime statistics for any
14 location(s);

15 (4) An assessment identifying any potential impact on civil liberties and civil rights and
16 discussing any plans to safeguard the rights of the public;

17 (5) The fiscal costs for the Surveillance Technology, including initial purchase,
18 personnel and other ongoing costs, and any current or potential sources of funding;

19 (6) Whether use or maintenance of the technology will require data gathered by the
20 technology to be handled or stored by a third-party vendor on an ongoing basis; and

21 (7) A summary of the experience, if any, other governmental entities have had with the
22 proposed technology, including information about its effectiveness and any known adverse information
23 about the technology such as unanticipated costs, failures, or civil rights and civil liberties abuses.

24 "Personal communication device" means a cellular telephone that has not been modified
25 beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or

1 similar wireless two-way communications and/or portable Internet accessing devices, whether
2 procured or subsidized by a City entity or personally owned, that is used in the regular course of
3 conducting City business.

4 “Surveillance Technology” means any software, electronic device, system utilizing an
5 electronic device, or similar device used, designed, or primarily intended to collect, retain, process, or
6 share audio, electronic, visual, location, thermal, biometric, olfactory or similar information
7 specifically associated with, or capable of being associated with, any individual or group. Surveillance
8 Technology” includes but is not limited to the following: international mobile subscriber identity
9 (IMSI) catchers and other cell site simulators; automatic license plate readers; electric toll readers;
10 closed-circuit television cameras; gunshot detection hardware and services; video and audio
11 monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and
12 wearable body cameras; mobile DNA capture technology; biometric software or technology, including
13 facial, voice, iris, and gait-recognition software and databases; software designed to monitor social
14 media services; x-ray vans; software designed to forecast criminal activity or criminality; radio-
15 frequency I.D. (RFID) scanners; and tools, including software and hardware, used to gain
16 unauthorized access to a computer, computer service, or computer network. Surveillance Technology
17 does not include the following devices, hardware, or software:

18 (1) Office hardware, such as televisions, computers, credit card machines, copy
19 machines, telephones, and printers, that are in common use by City Departments and used for routine
20 City business and transactions;

21 (2) City databases and enterprise systems that contain information kept in the ordinary
22 course of City business, including, but not limited to, human resource, permit, license, and business
23 records;

1 (3) City databases and enterprise systems that do not contain any data or other
2 information collected, captured, recorded, retained, processed, intercepted, or analyzed by
3 Surveillance Technology, including payroll, accounting, or other fiscal databases;

4 (4) Information technology security systems, including firewalls and other cybersecurity
5 systems intended to secure City data;

6 (5) Physical access control systems, employee identification management systems, and
7 other physical control systems;

8 (6) Infrastructure and mechanical control systems, including those that control or
9 manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;

10 (7) Manually-operated technological devices used primarily for internal City
11 communications, which are not designed to surreptitiously collect surveillance data, such as radios,
12 personal communication devices, and email systems;

13 (8) Manually-operated and non-wearable handheld cameras, audio recorders, and video
14 recorders, that are not designed to be used surreptitiously and whose functionality is limited to
15 manually capturing and manually downloading video and/or audio recordings;

16 (9) Surveillance devices that cannot record or transmit audio or video or be remotely
17 accessed, such as image stabilizing binoculars or night vision equipment;

18 (10) Computers, software, hardware, or devices, used in monitoring the work
19 and work-related activities involving City buildings, employees, contractors, and volunteers or
20 used in conducting internal investigations involving City employees, contractors, and
21 volunteers;

22 (4110) Medical equipment and systems used to record, diagnose, treat, or prevent
23 disease or injury, and used and/or kept in the ordinary course of providing City services;

24 (4211) Parking Ticket Devices;

1 (4312) Police Department interview rooms, holding cells, and internal security
2 audio/video recording systems;

3 (4413) Police department computer aided dispatch (CAD), records/case management,
4 Live Scan, booking, Department of Motor Vehicles, California Law Enforcement Telecommunications
5 Systems (CLETS), 9-1-1 and related dispatch and operation or emergency services systems;

6 (4514) Police department early warning systems; and

7 (4615) Computers, software, hardware, or devices intended to be used solely to
8 monitor the safety and security of City facilities and City vehicles not generally accessible to the
9 public, and their occupants.

10 "Surveillance Technology Policy" means a written policy that includes:

11 (1) A description of the product and services addressed by the Surveillance Technology,
12 including manufacturer and model numbers and/or the identity of any provider(s) whose services are
13 essential to the functioning or effectiveness of the Surveillance Technology equipment or services for
14 the intended purpose;

15 (2) A description of the purpose(s) for which the Surveillance Technology equipment or
16 services are proposed for acquisition, including the type of data that may be collected by the
17 Surveillance Technology equipment or services;

18 (3) The uses that are authorized, the rules and processes required prior to such use, and
19 uses of the Surveillance Technology that will be expressly prohibited.

20 (4) A description of the formats in which information collected by the Surveillance
21 Technology is stored, copied, and/or accessed;

22 (5) The specific categories and titles of individuals who are authorized by the
23 Department to access or use the collected information, including restrictions on how and under what
24 circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the
25 rules and processes required prior to access or use of the information;

1 (6) The general safeguards that protect information from unauthorized access, including
2 encryption and access control mechanisms;

3 (7) The limited time period, if any, that information collected by the Surveillance
4 Technology will be routinely retained, the reason such retention period is appropriate to further the
5 purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is
6 regularly deleted after that period lapses, and the specific conditions that must be met to retain
7 information beyond that period;

8 (8) How collected information can be accessed or used by members of the public,
9 including criminal defendants;

10 (9) Which governmental agencies, departments, bureaus, divisions, or units that may
11 receive data collected by the Surveillance Technology operated by the Department, including any
12 required justification or legal standard necessary to share that data and how it will ensure that any
13 entity receiving such data complies with the Surveillance Technology Policy;

14 (10) The training required for any individual authorized to use the Surveillance
15 Technology or to access information collected by the Surveillance Technology;

16 (11) The mechanisms to ensure that the Surveillance Technology Policy is followed,
17 including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of
18 the use of the technology or access to information collected by the technology, technical measures to
19 monitor for misuse, any independent person or entity with oversight authority, and the sanctions for
20 violations of the policy; and

21 (12) What procedures will be put in place by which members of the public can register
22 complaints or concerns, or submit questions about the deployment or use of a specific Surveillance
23 Technology, and how the Department will ensure each question and complaint is responded to in a
24 timely manner.

1 SEC. 19B.2. BOARD OF SUPERVISORS APPROVAL OF SURVEILLANCE

2 TECHNOLOGY POLICY.

3 (a) Except as stated in subsection (c), and in accordance with the procedures set forth in
4 subsection (b), a Department must obtain Board of Supervisors approval by ordinance of a
5 Surveillance Technology Policy under which the Department will acquire and use Surveillance
6 Technology, prior to engaging in any of the following:

7 (1) Seeking funds for Surveillance Technology, including but not limited to applying for
8 a grant, or accepting state or federal funds, or public or private in-kind or other donations;

9 (2) Acquiring or borrowing new Surveillance Technology, including but not limited to
10 acquiring Surveillance Technology without the exchange of monies or other consideration;

11 (3) Using new or existing Surveillance Technology for a purpose, in a manner, or in a
12 location not specified in a Surveillance Technology Policy ordinance approved by the Board in
13 accordance with this Chapter 19B; or

14 (4) Entering into agreement with a non-City entity to acquire, share, or otherwise use
15 Surveillance Technology;

16 (5) Entering into an oral or written agreement under which a non-City entity or
17 individual regularly provides the Department with data or information acquired through the
18 entity's use of Surveillance Technology.

19 (b) The Board of Supervisors may approve a Surveillance Technology Policy ordinance
20 under subsection (a) only under the following circumstances:

21 (1) The Department seeking Board approval under subsection (a) first submits to
22 COIT a Surveillance Impact Report for the Surveillance Technology to be acquired or used;

23 (2) Based on the Surveillance Impact Report submitted by the Department,
24 COIT develops a Surveillance Technology Policy for the Surveillance Technology to be
25 acquired or used;

1 (3) At a public hearing at which COIT considers the Surveillance Technology
2 Policy, COIT recommends that the Board of Supervisors adopt, adopt with modifications, or
3 decline to adopt the Surveillance Technology Policy for the Surveillance Technology to be
4 acquired or used.

5 (c) A Department is not required to obtain Board of Supervisors approval by ordinance
6 of a Surveillance Technology Policy if the Department's acquisition or use of the Surveillance
7 Technology complies with a Surveillance Technology Policy previously approved by the Board
8 by ordinance.

9 (d) Notwithstanding the provisions of this Chapter 19B, it shall be unlawful for any Department
10 to obtain, retain, access, or use: 1) any Face Recognition Technology; or 2) any information obtained
11 from Face Recognition Technology. A Department's inadvertent or unintentional receipt, retention
12 access to, or use of any information obtained from Face Recognition Technology shall not be
13 a violation of this subsection (b), provided that:

14 (1) The Department does not request or solicit its receipt, access to, or use of
15 such information; and

16 (2) The Department logs such receipt, access to, or use in its Annual
17 Surveillance Report.

18 (ee) If either the District Attorney or Sheriff certifies in writing to the Controller that
19 acquisition of Surveillance Technology is necessary to perform an investigative or prosecutorial
20 function and provides in writing to the Controller either an explanation of how compliance with this
21 Chapter 19B will obstruct their investigative or prosecutorial function or a declaration that the
22 explanation itself will obstruct either function, the District Attorney or Sheriff shall simultaneously
23 submit a copy of the document to the Clerk of the Board of Supervisors so that the Board in its
24 discretion may hold a hearing and request that the District Attorney or Sheriff appear to respond to the
25

1 Board's questions regarding such certification, explanation, and/or declaration. The written
2 certification shall specify the Surveillance Technology acquired, or to be acquired.

3 (df) Nothing in this Chapter 19B shall be construed to obstruct the constitutional and statutory
4 powers and duties of the District Attorney, the Sheriff, the Chief Adult Probation Officer, or the Chief
5 Juvenile Probation Officer.

6 (g) Nothing in this Chapter 19B shall be construed to prohibit, restrict, or interfere with
7 the receipt by a City department of information gathered by a non-City entity or individual from
8 Surveillance Technology, provided that the Department's receipt of the information would not
9 otherwise violate this Chapter 19B.

10
11 **SEC. 19B.3. SURVEILLANCE IMPACT REPORT AND SURVEILLANCE TECHNOLOGY**
12 **POLICY SUBMISSION.**

13 (a) COIT shall post on COIT's website each Surveillance Impact Report submitted by
14 Departments under subsection 19B.2(b)(1) and COIT's recommendations to the Board of
15 Supervisor's under subsection 19B.2(b)(3) for each Surveillance Technology Policy.

16 (ab) The Department seeking approval under Section 19B.2 shall submit to the Board of
17 Supervisors and publicly post on the Department website a Surveillance Impact Report and a proposed
18 Surveillance Technology Policy ordinance at least 30 days prior to the public meeting where the Board
19 will consider that Surveillance Technology Policy ordinance pursuant to Section 19B.2.

20 (bc) Prior to submitting the Surveillance Technology Policy ordinance to the Board, the
21 Department must first approve the policy, submit the policy to the City Attorney for review, and submit
22 the policy to the Mayor.

23
24 **SEC. 19B.4. STANDARD FOR APPROVAL.**
25

1 It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy
2 ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes
3 outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and
4 civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will
5 not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any
6 community or group.

7
8 **SEC. 19B.5. COMPLIANCE FOR EXISTING SURVEILLANCE TECHNOLOGY.**

9 (a) Each Department possessing or using Surveillance Technology before the effective date of
10 this Chapter 19B shall submit an inventory of its Surveillance Technology to COIT, within 60
11 days of the effective date of this Chapter. COIT shall publicly post the inventory on COIT's
12 website.

13 (b) Each Department possessing or using Surveillance Technology before the effective
14 date of this Chapter 19B shall submit a proposed Surveillance Technology Policy ordinance to the
15 Board of Supervisors, in accordance with the procedures set forth in subsection 19B.2(b), for
16 that each particular Surveillance Technology no later than 120 days following the effective date of this
17 Chapter, for review and approval by the Board by ordinance.

18 (c) If a Department is unable to meet this 120-day timeline, the Department may notify the
19 Clerk of the Board of Supervisors in writing of the Department's request to extend this period and the
20 reasons for that request. The Clerk of the Board may for good cause grant a Department a single
21 extensions of up to 90 days per extension, beyond the 120-day timeline to submit a proposed
22 Surveillance Technology Policy.

23 (d) If the Board has not approved a Surveillance Technology Policy ordinance for
24 Surveillance Technology in use before the effective date of this Chapter 19B, within 180 days of its
25 submission to the Board, the Department shall cease its use of the Surveillance Technology and the

1 sharing of data from the Surveillance Technology until such time as the Board approves the
2 Surveillance Technology Policy ordinance in accordance with this Chapter.

3
4 **SEC. 19B.6. ANNUAL SURVEILLANCE REPORT.**

5 (a) A Department that obtains approval for the acquisition of Surveillance Technology under
6 Section 19B.2 must submit to the Board of Supervisors and COIT, and make available on its website,
7 an Annual Surveillance Report for each Surveillance Technology used by the City Department within
8 12 months of Board approval of the applicable Surveillance Technology Policy, and annually
9 thereafter on or before November 1. If the Department is unable to meet the deadline, the Department
10 may submit a request to the Clerk of the Board for an extension of the deadline. The Clerk may extend
11 the deadline for good cause.

12 (b) By no later than January 15 of each fiscal-year, each Department that has obtained
13 approval for the acquisition of Surveillance Technology under Section 19B.2 shall submit to the Board
14 of Supervisors the Department's Annual Surveillance Report a report regarding implementation
15 of the policy and a resolution to accept the report.

16 (c) By no later than January 15 of each year, the Board of Supervisors shall publish a summary
17 of all requests for Board approval of Surveillance Technology Policy ordinances, which shall include a
18 summary of any Board action related to such requests, and all Annual Surveillance Reports submitted
19 in the prior calendar year.

20 (d) By no later than January 15 of each year, COIT shall post on its website each
21 Annual Surveillance Report submitted to COIT in the prior year.

22
23 **SEC. 19B.7. USE OF SURVEILLANCE TECHNOLOGY IN EXIGENT**
24 **CIRCUMSTANCES.**

1 (a) A Department may temporarily acquire or temporarily use Surveillance Technology in
2 exigent circumstances without following the provisions of this Chapter 19B. If a Department acquires
3 or uses Surveillance Technology under this Section 19B.7, the Department shall do all of the following:

4 (1) Use the Surveillance Technology solely to respond to the exigent circumstances;

5 (2) Cease using the Surveillance Technology within seven days, or when the exigent
6 circumstances end, whichever is sooner;

7 (3) Keep and maintain only data related to the exigent circumstances, and dispose of
8 any data that is not relevant to an ongoing investigation, unless its retention is (A) authorized by a
9 court based on a finding of probable cause to believe the information constitutes evidence of a crime;
10 or (B) otherwise required by law;

11 (4) Not disclose to any third party any information acquired during exigent
12 circumstances unless such disclosure is (A) authorized by a court based on a finding of probable cause
13 to believe the information constitutes evidence of a crime; or (B) otherwise required by law; and

14 (5) Submit a written report summarizing that acquisition and/or use of Surveillance
15 Technology under this Section 19B.7 to the Board of Supervisors within 45 days following the inception
16 of the exigent circumstances.

17 (b) Any Surveillance Technology temporarily acquired in exigent circumstances shall be
18 returned within 7 days following its acquisition, or when the exigent circumstances end, whichever is
19 sooner, unless the Department acquires the Surveillance Technology in accordance with the
20 requirements of this Chapter 19B.

21
22 **SEC. 19B.8. ENFORCEMENT.**

23 (a) If a Department alleged to have violated this Chapter 19B takes corrective measures in
24 response to such allegation, the Department shall post a notice on the Department's website that
25 generally describes any corrective measure taken to address such allegation.

1 (b) ~~It shall be a misdemeanor to knowingly use City-owned Surveillance Technology (1)~~
2 ~~for a purpose or in a manner that is specifically prohibited in a Board-approved Surveillance~~
3 ~~Technology Policy ordinance, or (2) without complying with the terms of this Chapter 19B.~~
4 ~~Unless otherwise prohibited by law, the District Attorney may prosecute a violation of this~~
5 ~~Chapter.~~

6 (eb) Any violation of this Chapter 19B constitutes an injury and any person may institute
7 proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent
8 jurisdiction to enforce this Chapter 19B. An action instituted under this subsection (c) shall be brought
9 against the City.

10 (ec) Prior to the initiation of any legal proceeding under subsection (c), the City must be given
11 written notice of the violation(s) and an opportunity to correct such alleged violation(s) within 30 days
12 of receipt of the notice.

13 (ed) If the alleged violation(s) is substantiated and subsequently corrected, a notice shall be
14 posted in a conspicuous space on the City's website that describes the corrective measure(s) taken to
15 address the violation(s).

16 (fe) A court shall award costs and reasonable attorney's fees to a plaintiff who is a prevailing
17 party in any action brought under subsection (c).

18
19 Section 3. The Administrative Code is hereby amended by revising Sections 2A.20 and
20 10.170-1, and adding Sections 3.27 and 21.07, to read as follows:

21
22 **SEC. 2A.20. CONTROLLER'S AUDITS.**

23 (a) The Controller shall audit the accounts of all boards, officers, and employees of the
24 City and County charged in any manner with the custody, collection, or disbursement of funds.
25

1 The Controller shall audit all accounts of money coming into the hands of the Treasurer, the
2 frequency of which shall be governed by State law.

3 (b) The Controller shall have the authority to audit the operations of all boards,
4 commissions, officers, and departments to evaluate their effectiveness and efficiency. The
5 Controller shall have access to, and authority to examine all documents, records, books, and
6 other property of any board, commission, officer, or department.

7 (c) When requested by the Mayor, the Board of Supervisors, or any board or
8 commission for its own department, the Controller shall audit the accounts of any officer or
9 department.

10 (d) Surveillance Technology Audit.

11 (1) For purposes of this subsection (d), "Department," "Surveillance Technology,"
12 "Surveillance Technology Policy," and "Annual Surveillance Report" have the meanings set forth in
13 Section 19B.1 of the Administrative Code.

14 (2) Acting as City Services Auditor, and beginning in fiscal year 2019-2020, the
15 Controller shall audit annually the use of Surveillance Technology by Departments. Such an audit shall
16 include a review of whether a Department has operated and is operating in compliance with an
17 approved Surveillance Technology Policy ordinance, and has completed an Annual Surveillance
18 Report. The audit shall also include a review of the difference, if any, between the full cost of the
19 Surveillance Technology equipment and services included in the Surveillance Technology Policy and
20 the total annual costs for the Surveillance Technology included in the Annual Surveillance Report. At
21 the completion of the audit and in consultation with the City Attorney, the Controller shall recommend
22 any changes to any Surveillance Technology Policy ordinance and its implementation to the Board of
23 Supervisors.

24
25 **SEC. 10.170-1. GRANT FUNDS – ACCEPTANCE AND EXPENDITURE.**

1 (a) Any department, board, or commission that seeks to accept and expend federal,
2 State, or other grant funds must comply with any applicable provisions of this Section 10.170-
3 1.

4 (b) The acceptance and expenditure of federal, State, or other grant funds in the
5 amount of \$100,000 or more is subject to the approval by resolution of the Board of
6 Supervisors. If, as a condition of the grant, the City is required to provide any matching funds,
7 those funds shall be included in determining whether the grant meets the \$100,000 threshold.
8 This subsection (b) shall also apply to an increase in a grant where the increase, alone or in
9 combination with any other previous increases to that grant, would raise the cumulative total
10 amount of the grant to \$100,000 or more. The department, board, or commission requesting
11 approval shall submit the following documents to the Board prior to its consideration:

12 (1) A proposed resolution approving the acceptance and expenditure of grant
13 funds, or a proposed ordinance as required under subsection (d), signed by the department
14 head, the Mayor or his or her designee, and the Controller;

15 (2) A completed "Grant Information Form." The Clerk of the Board shall prepare
16 the form; it shall include a disability access checklist, indirect cost recovery, and other
17 information as the Board of Supervisors may require;

18 (3) A copy of the grant application;

19 (4) A letter of intent to award the grant or acknowledgment of grant award from
20 the granting agency; and,

21 (5) A cover letter to the Clerk of the Board ~~of Supervisors~~ substantially conforming
22 to the specifications of the Clerk of the Board.

23 (c) Grants or Increases to Grants of Less Than \$100,000. The Controller may prescribe
24 rules for the acceptance and expenditure of federal, State, or other grant funds in amounts
25 less than \$100,000, or for increases to grants where the increase, alone or in combination

1 with any other previous increases to that grant, would not raise the cumulative total amount of
2 the grant to \$100,000 or more. The Controller may also prescribe rules for the acceptance
3 and expenditure of increases to grants, where the original grant or any subsequent increase
4 to the grant has been approved by the Board of Supervisors under subsection (b) or (d) and
5 where the latest increase would be in an amount less than \$50,000.

6 * * * *

7 (l) Surveillance Technology.

8 (1) For purposes of this subsection (l), "Department," "Surveillance Technology," and
9 "Surveillance Technology Policy" have the meanings set forth in Section 19B.1 of the Administrative
10 Code.

11 (2) Notwithstanding the provisions of subsections (b) and (c) above, when any City
12 official, Department, board, commission or other entity of the City (collectively, the "requesting
13 department") seeks authority to apply for, accept, or expend federal, State, or other grant funds in any
14 amount to purchase Surveillance Technology, the requesting department must submit a Surveillance
15 Technology Policy, approved by the Board of Supervisors in accordance with Chapter 19B of the
16 Administrative Code, to the Board of Supervisors with a request for authorization to accept and expend
17 grant funds.

18
19 **SEC. 3.27. APPROPRIATIONS FOR SURVEILLANCE TECHNOLOGY.**

20 (a) For purposes of this Section 3.27, "Department," "Surveillance Technology," and
21 "Surveillance Technology Policy" have the meanings set forth in Section 19B.1 of the Administrative
22 Code.

23 (b) To the extent that a Department seeks funding to acquire Surveillance Technology, the
24 Department shall transmit a Surveillance Technology Policy, approved by the Board of Supervisors in
25 accordance with Chapter 19B of the Administrative Code, with any budget estimate submitted to the

1 Controller in accordance with Section 3.3(a) or 3.15 of the Administrative Code. To the extent the
2 Mayor concurs in the funding request and the Surveillance Technology Policy, the Mayor shall include
3 the Surveillance Technology Policy with the proposed budget submitted to the Board of Supervisors in
4 accordance with Section 3.3(c) or (d) of the Administrative Code, or, in the case of a supplemental
5 appropriation, Section 3.15 of the Administrative Code.

6 ##

7 **SEC. 21.07. ACQUISITION OF SURVEILLANCE TECHNOLOGY.**

8 (a) For purposes of this Section 21.07, "Department," "Surveillance Technology," and
9 "Surveillance Technology Policy" have the meanings set forth in Section 19B.1 of the Administrative
10 Code.

11 (b) Notwithstanding any authority set forth in this Chapter 21, neither the Purchaser nor any
12 Contracting Officer may acquire any Surveillance Technology unless the Board of Supervisors has
13 appropriated funds for such acquisition in accordance with the requirements of Chapter 19B of the
14 Administrative Code.

15
16 Section 4. The Administrative Code is hereby amended by revising Chapter 22A,
17 Section 22A.3 as follows:

18
19 **SEC. 22A.3. COMMITTEE ON INFORMATION TECHNOLOGY.**

20
21 * * * *

22 (k) When a City Department submits to COIT a Surveillance Impact Report under
23 subsection 19B.2(b)(1) of Chapter 19B of the Administrative Code, COIT shall develop a
24 Surveillance Technology Policy for the Department. For purposes of this subsection (k), "City
25

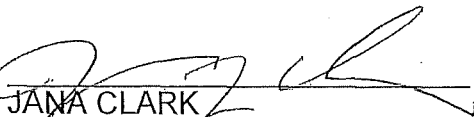
1 Department,” “Surveillance Technology Policy,” and “Surveillance Impact Report” shall have
2 the meanings set forth in Section 19B.1 of Chapter 19B of the Administrative Code.

3
4 Section 5. Effective Date. This ordinance shall become effective 30 days after
5 enactment. Enactment occurs when the Mayor signs the ordinance, the Mayor returns the
6 ordinance unsigned or does not sign the ordinance within ten days of receiving it, or the Board
7 of Supervisors overrides the Mayor’s veto of the ordinance.

8 Section 6. Scope of Ordinance. In enacting this ordinance, the Board of Supervisors
9 intends to amend only those words, phrases, paragraphs, subsections, sections, articles,
10 numbers, punctuation marks, charts, diagrams, or any other constituent parts of the Municipal
11 Code that are explicitly shown in this ordinance as additions, deletions, Board amendment
12 additions, and Board amendment deletions in accordance with the “Note” that appears under
13 the official title of the ordinance.

14
15
16 APPROVED AS TO FORM:
17 DENNIS J. HERRERA, City Attorney

18 By:


19 JANA CLARK
20 Deputy City Attorney

21 n:\leganalas2019\1900073\01354576.docx

LEGISLATIVE DIGEST
(Revised 04/22/19)

[Administrative Code - Acquisition of Surveillance Technology]

Ordinance amending the Administrative Code to require that City departments acquiring Surveillance Technology, or entering into agreements to receive information from non-City owned Surveillance Technology, submit a Board of Supervisors approved Surveillance Technology Policy Ordinance, based on a policy developed by the Committee on Information Technology (COIT), and a Surveillance Impact Report to the Board in connection with any request to appropriate funds for the purchase of such technology or to accept and expend grant funds for such purpose, or otherwise to procure Surveillance Technology equipment or services; require each City department that owns and operates existing surveillance technology equipment or services to submit to the Board a proposed Surveillance Technology Policy Ordinance governing the use of the surveillance technology; and requiring the Controller, as City Services Auditor, to audit annually the use of surveillance technology equipment or services and the conformity of such use with an approved Surveillance Technology Policy Ordinance and provide an audit report to the Board of Supervisors.

Existing Law

Existing law requires any department, board or commission that seeks to accept and expend grant funds in excess of \$100,000 to request Board of Supervisors' approval. Existing law requires any department, board or commission that seeks to accept and expend grant funds less than \$100,000 to comply with rules prescribed by the Controller for the acceptance and expenditure of grant funds.

Existing law requires that any department, board or commission that seeks to purchase commodities and services comply with the Purchaser's rules and regulations set forth in Chapter 21 of the Administrative Code.

Existing law requires that the Controller audit the accounts of all boards, officers and employees and the account of all moneys coming into the hands of the Treasurer. Existing law authorizes the Controller to audit the effectiveness and efficiency of all boards, commissions, officers and departments.

Amendments to Current Law

This ordinance would require departments (defined to exclude the District Attorney and Sheriff while performing investigative or prosecutorial functions) seeking to acquire surveillance

technology or services; or to enter into agreements to receive information gathered by non-City entities from surveillance technology, to submit to the Committee on Information Technology (COIT), a Surveillance Impact Report. This ordinance would require COIT to develop a Surveillance Technology Policy. This ordinance would require that a Surveillance Technology Policy describe the product or services, their purpose and cost, locations for use, a data storage and retention plan, authorized uses, whether the data will be public, authorized access, required training, access controls, complaint procedures, and any safeguards to reduce the chilling effect of the technology and prevent its unauthorized use. This ordinance would prohibit departments' use of surveillance technology services or equipment, or departments' receipt of data from non-City Surveillance Technology, unless the Board of Supervisors had approved a Surveillance Technology Policy ordinance for the use of services or equipment, or receipt of that information, following COIT's development of a policy and recommendation. This ordinance would require departments seeking to acquire surveillance technology or services to submit with any funding request a Surveillance Technology Policy ordinance, approved by the Board of Supervisors. It also would require that departments prepare for review by the Board of Supervisors an Annual Surveillance Report that describes how the technology was used, what data was retained, deleted, or shared, a summary of public comments or concerns about the technology's use, the results of any internal audit, statistics that calculate its effectiveness in achieving its designed purpose, whether data generated was requested and or provided by and to the public, and the total costs. This ordinance would prohibit departments' use of face recognition technology, except at federally regulated facilities at the Airport or Port.

The ordinance also would require the Controller to audit annually the use of surveillance technology, including a review of whether a department has and is operating in compliance with a Surveillance Technology Policy ordinance and completed an Annual Surveillance Report. The ordinance also would require that the Controller's audit include a review of the costs of the surveillance technology and services. Finally, the ordinance would require that the Controller, in consultation with the City Attorney, recommend any changes to any Surveillance Technology Policy ordinance and its implementation to the Board of Supervisors.

Background Information

This ordinance reflects amendments made at the April 22, 2019 meeting of the Rules Committee. This ordinance was amended to modify the definition of surveillance technology to include technology used to monitor or investigate City employees or contractors. This ordinance was amended to require certain procedures be followed before the Board may approve a Surveillance Technology Policy ordinance: (1) Departments must first submit to COIT a Surveillance Impact Report for the Surveillance Technology to be acquired or used; (2) COIT must develop a Surveillance Technology Policy for the Surveillance Technology to be acquired or used; and (3) Following a public hearing at which COIT considers the Surveillance Technology Policy, COIT must recommend that the Board adopt, adopt with modifications, or decline to adopt the Surveillance Technology Policy. This ordinance also

FILE NO. 190110

was amended to require that departments obtain Board approval by ordinance of a Surveillance Technology Policy before entering into an agreement under which a non-City entity regularly provides data or information acquired through the entity's use of surveillance technology. This ordinance also was amended to permit the use of face recognition technology at federally-regulated facilities at the Airport and Port and to clarify that the unintentional or inadvertent receipt or use of face recognition technology does not violate the prohibition on the use or receipt of that technology. Finally, this ordinance was amended to delete language making knowing use of surveillance technology a misdemeanor.

n:\legana\as2019\1900073\01354577.docx

Young, Victor (BOS)

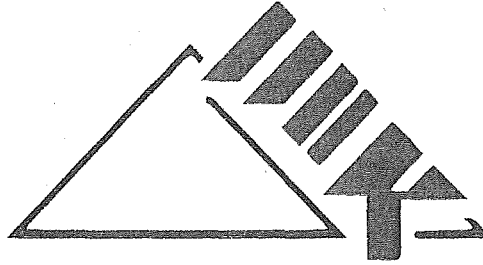
From: RivamonteMesa, Abigail (BOS)
Sent: Monday, April 15, 2019 11:49 AM
To: BOS Legislation, (BOS); Young, Victor (BOS)
Cc: Haney, Matt (BOS); Peskin, Aaron (BOS); Hepner, Lee (BOS)
Subject: Co-Sponsor 190110 Acquisition of Surveillance Technology

Hello,

Supervisor Haney would like to co-sponsor 190110 Acquisition of Surveillance Technology

Thank you,
Abigail

Abigail Rivamonte Mesa
Office of Supervisor Matt Haney, D6
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, CA 94102
T 415-554-7969 | F 415-554-7974
abigail.rivamontemesa@sfgov.org | www.sfbos.org



**Golden Gate Heights Neighborhood Association
P.O. Box 27608
San Francisco, CA 94127**

Norman Yee, President, Board of Supervisors
City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, Ca 94102-4689

April 1, 2019

Re: Proposed Video Surveillance Ordinance; Pursuant to Proposition B (2018)

Dear Supervisor Yee,

We are writing to express our strong opposition to the proposed Video Surveillance Ordinance, as currently written, and to suggest that the Board of Supervisors make the changes recommended by StopCrimeSF (see attached) before passage of this enabling legislation.

As citizens of San Francisco, we believe that the potential mis-use by government or private entities of technology to invade the privacy or abuse the civil liberties of Americans or visitors requires constant vigilance. The passage of Proposition B (2018) by voters is an important step in this regard.

However, as sadly demonstrated in a host of countries around the world, individual criminal activity and organized crime can have a greater impact on citizens' sense of security and their very freedom than government abuse. Indeed, a major, if not the major, role of local government is to provide an environment in which citizens can live with freedom from fear and feeling secure in their persons and property.

Sadly, San Francisco is no longer such a place. As you know, we have an epidemic of property crime in our City, including auto and home burglaries, the former being one of the highest rates in the nation, among comparable cities. Tourists and visitors are regularly preyed upon, to the point that national and international news stories have featured the issue and major organizations have cancelled planned conventions in the City. This has potentially massive economic impact on businesses and residents, who depend on the dollars spent here by visitors who, like residents, should feel safe on our streets and in their dwellings.

Although San Francisco's violent crime rate is lower than some comparable cities, an environment in which property crime thrives is often a precursor to violent incidents. We have already seen this, as evidenced by the recent brutal beating of an elderly woman during the commission of a home invasion robbery, or the killing of a photographer in broad daylight on Twin Peaks by someone attempting to steal his camera. In our neighborhood recently, there have been several armed robberies of individuals on their way to work in early morning daylight hours. Any of these could have resulted in tragedy and all make residents feel unsafe.

Video surveillance and other technologies such as GPS, license plate recognition, gunfire detection technologies and others play an essential role in capturing suspects and assisting in their conviction for crimes. This not only takes individual criminals off the streets, but facilitates breaking up organized crime gangs, and creates an environment which signals to potential criminals that San Francisco cares about the safety of its citizens and visitors and will act effectively to assure it, thus preventing crime in the first place.

We believe the Board of Supervisors has the responsibility and the latitude, based on the text of Proposition B, to use their judgment to balance legitimate concerns about the abuse of technology, with the need to use today's technology, today, to assure the safety and well-being of their constituents and visitors to San Francisco. The proposed Ordinance goes too far, too fast in several important areas, which are cogently outlined in the StopCrimeSF document attached.

We believe StopCrimeSF's recommendations are reasonable and if enacted, will enable the Board of Supervisors to best discharge their obligations to simultaneously prevent the abuse of technology, as well as to address the growing concerns of both residents and visitors about their safety in their homes, hotels and on the streets of San Francisco.

We urge you to adopt the StopCrimeSF recommendations.

Sincerely,

The Golden Gate Heights Neighborhood Association
Sally Stephens, President

CC:
London Breed, Mayor, San Francisco
William Scott, Chief of Police, San Francisco
George Gascón, District Attorney, San Francisco
StopCrimeSF

Attachment: StopCrimeSF recommended changes to Video Surveillance Ordinance



STOP CRIME SF

Neighborhoods for Criminal Justice Accountability

Dear President Yee,

Stop Crime SF represents more than 500 San Francisco residents working together to reduce and prevent crime in our neighborhoods while holding public officials and the criminal justice system accountable. We run a Court Watch program to ensure our elected judges take crime seriously. We also facilitate the installation of video security cameras in business and residential areas with private donations and city grants such as your Participatory Budgeting program.

These camera installations in neighborhoods like Golden Gate Heights, Bayview and the West Portal business district are popular with residents and merchants. San Francisco police officers and assistant district attorneys tell us the cameras provide valuable video evidence for arresting and convicting burglars. Video is an important tool to tackle property crime in San Francisco, which has the highest rate of property crime of the nation's most populated cities.

We are concerned about the so-called "Stop Secret Surveillance Ordinance" currently being considered by the Board of Supervisors. It will significantly limit the ability of law enforcement to fight crime with video cameras.

The proposed ordinance would:

1. Prohibit city departments from using security technology services or equipment unless the Board of Supervisors first approves a Surveillance Technology policy for the services and equipment.
2. Outright ban the use of facial recognition technology.

We understand the good intentions of the legislation. No one can pretend that facial recognition technology is perfect, especially when it has trouble properly identifying people of color. The FBI's facial recognition technology had a 14 percent failure rate as of 2016, according to a U.S. General Accounting Office report. While that is undoubtedly better than visual identification by victims or bystanders, it cannot be the sole factor in arrests. But combined with good police work and when deployed in conjunction with well-crafted public policy, it can serve as a useful tool. A ban precludes any thoughtful regulation: It's just throwing the baby out with the bathwater.

An outright ban also precludes the possibility of significant technological improvements, just as has occurred in DNA identification in recent years. The software has already advanced by leaps and bounds in recent years, and much better accuracy may be around the corner. Refinements that address today's shortcomings could make facial recognition a valuable security tool.

Our greatest concern with the proposed legislation is how it will affect the use of traditional security video. The expense and burden of the ordinance's required audits and reports — not to mention approval from the full Board of Supervisors — would make it much more difficult to set up or continue operation of city-operated security cameras in timely fashion in San Francisco.

What about security cameras on private homes and businesses? The proposed law doesn't restrict a private citizen from installing a camera. But the ordinance would seemingly require the city to develop a use policy and receive Board of Supervisors approval before "entering into agreement with a non-city entity to acquire, share, or otherwise use surveillance technology."

This broad language could restrict the city from using information provided by any private citizen or local business that doesn't strictly adhere to the city's yet-to-be-developed policies. When a crime is committed, there should be no such restrictions on SFPD's access to information provided by the public which might help in an arrest of a violent or repeat offender.

Valuable video footage, such as that which captured the 2017 murder of photographer Ed French on Twin Peaks, could serve justice. Such footage might not exist in future cases if the ordinance curtails the use of city-operated cameras.

The law could also make it more difficult for San Francisco to partner with other law enforcement agencies. The politically charged Board of Supervisors would have to approve cooperation. The law has an exception that allows the city to use surveillance technology in emergencies for seven days. But is that enough time to thwart a terrorist attack?

After the Boston marathon bombing, more than 4,000 hours of police time were spent investigating terrorists. Surveillance video helps monitor areas without adequate police coverage. Video is also unbiased and provides total recall of events. We can save time, money and most importantly lives by effective use of surveillance technology as a force-multiplier.

San Francisco has its own marathon, and other high-profile events like the Pride and Chinese New Year parades that attract hundreds of thousands of people. Will these events become known as easy targets? As a city that stands for diversity, San Francisco is particularly

vulnerable to threats from anti-LGBTQ, white supremacist or other terrorists. We should not let our guard down.

Beyond cameras, the ordinance broadly applies to other essential public safety tools, including license-plate readers, gunshot-detection hardware, DNA-capture technology and radio-frequency-ID scanners. It would even affect the body cameras worn by police officers.

As nearby cities use the technology we seek to ban and limit, criminals will commute to San Francisco as the place where they can conduct their criminal activities unnoticed. They already flock to San Francisco to break into cars because they think our judges, juries and prosecutors don't take property crime as seriously as other cities.

Nothing in current law now prevents the Board of Supervisors and the agencies from creating policies governing the acquisition or use of security cameras and related technology. To put the cart before the horse jeopardizes public safety for no valid reason. The Board should proceed to adopt reasonable policies forthwith, but without requiring a halt to ongoing necessary operations while such policies are considered.

The Board of Supervisors should continue this hearing until it has first completed a study on this issue and received input from the District Attorney, police department and other agencies, all of which have expertise on such technologies. Then a hearing should be held by the Police Commission or other relevant body with expertise, to allow the public to hear recommendations and comment on this issue.

We also submit below suggested amendments to this ordinance.

Please feel free to contact Stop Crime SF president Frank Noto at 415-830-1502 if you have any questions.

Sincerely,

Frank Noto
Joel Engardio
Alice Xavier

Stop Crime SF

Suggested amendments:

- **Exclude the District Attorney, Sheriff and Police Departments (while performing investigative, prosecutorial or security functions, including terrorist and hate-crime threats) from the requirements of this ordinance.**

The proposed ordinance would require the SFPD to cease use of vehicular or body-mounted cameras during operations within 120 days unless and until both the department and the Board of Supervisors comply with certain requirements; this could result in an increase in unsolved crimes, police misconduct, or misidentification of innocent members of the public. Similarly, the Sheriff's Department could not monitor operations in the prisons, or the DA use video/photo evidence to prosecute domestic violence or other violent crime cases. Failure to permit monitoring in the prisons could result in prisoner abuse or prisoner-on-prisoner violence, while limitations on access by the DA could result in miscarriages of justice and increase the crime rate. San Francisco juries increasingly seldom convict in property crimes without photographic evidence.

- **Exclude SFO from certain requirements of this ordinance.**
It is intuitively obvious that airports are particularly vulnerable to certain types of terrorist activity.
- **Change the effective date of the Ordinance to the beginning of the next fiscal year, or 180 days after enactment, whichever comes later.**
Most departments do not have the expertise or resources to fulfil the detailed and highly technical requirements of this proposed legislation without additional time.
- **Require that additional funds be explicitly allocated to each affected department in the applicable fiscal year, including the Controllers' office, to comply with the requirements of this ordinance.**
Reducing existing services in order to comply with the proposed ordinance's requirements is unacceptable.
- **Revise compliance dates**
In Sec. 19.B.5 (a) to 180 days and in Sec. 19.B.5 (b) to 150 days, for reasons stated above.
- **Require any cost benefit analysis to include an estimate of economic and social costs to the public as well as city government of reduced arrests and convictions that might result from banned or restricted use of technology.**
- **Require any cost benefit analysis to examine the cost of alternatives to surveillance technology.**
- **Delete requirements for public release of identification of certain locations for surveillance technology.**
This information should be classified for selected locations to protect against criminal activity or terrorist activities. There is no reason to give potential lawbreakers a roadmap to areas where they can safely carry out criminal activities.

- **Eliminate any ban on facial recognition technology or include at minimum a two-year sunset clause in any such ban.**

This technology is improving at a rapid rate, so error rates will inevitably improve. Existing problems likely will diminish or disappear with technological advances, so further legislative action should be required if justified when examining future outcomes.

- **Clarify the definition of “any individual or group” included in the definition of “Surveillance Technology” to exclude criminals, suspects and prisoners.**

Obviously, the legitimate aim of surveillance is to identify and prevent these groups from the commission of crimes.

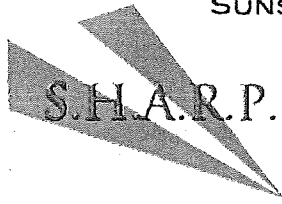
- **Consider the impacts on the public of reduced surveillance at large crowd events such as the Pride Parade and the Chinese Lunar New Year celebration.**

These events might become targets for hate-group terrorists if it became known that surveillance technology use was reduced at such occasions.

- **Allow the public to provide surveillance evidence to City agencies for use in crime investigations.**

- **Exempt use of facial recognition technology to access computer, smart phone and other instruments used by City employees.**

Rather than use passwords, many devices employ facial recognition to allow users access to their phones, etc.



SUNSET HEIGHTS ASSOCIATION OF RESPONSIBLE PEOPLE

WWW.SHARPSF.COM

San Francisco Board of Supervisors

RE: Surveillance Technology Ordinance - Rules Committee on April 15

Dear Supervisors,

The Sunset Heights Association of Responsible People (SHARP) is both a neighborhood association with more than 130 members and a foundation that provides grants that support dozens of San Francisco community organizations.

We are writing regarding the proposed Surveillance Technology Ordinance before the Rules Committee on April 15. While the intent to protect civil liberties is laudable, we believe the legislation needs further work because it could potentially impact the safety of everyone who visits and lives in San Francisco. This ordinance could affect local government and law enforcement's use of security cameras as well as other privately-owned security systems in San Francisco.

While we support reasonable policies to control surveillance technology, we recognize that criminal activity and organized crime can have a greater impact on citizens' sense of security and their very freedom than potential San Francisco government abuse. A key role of local government is to provide an environment in which citizens can live with freedom from fear and feel secure in their persons and property.

Video surveillance and other technologies such as GPS, license plate recognition, gunfire detection technologies and others play an essential role in capturing suspects and assisting in their conviction for crimes. This not only takes individual criminals off the streets, but facilitates breaking up criminal gangs large and small, and creates an environment which signals to potential criminals that San Francisco cares about the safety of its citizens and visitors and will act effectively to assure it, thus preventing crime in the future.

Such technology is also a force multiplier that aids law enforcement in preventing and discouraging terrorist incidents and apprehending those engaged in terrorist acts. Such acts might be aimed at major crowd events that celebrate San Francisco's diversity such as the Pride Parade, Lunar New Year and musical concerts in Golden Gate Park.

S.H.A.R.P. c/o 1661 7TH AVE. SAN FRANCISCO, CA 94122

The proposed law seemingly bans San Francisco residents and businesses from sharing security camera video or photos with the SFPD unless and until the Board enacts a camera policy. It explicitly prohibits City agencies from:

“entering into agreement with a non-city entity (e.g., a San Francisco resident or business) to acquire, share, or otherwise use surveillance technology.”

The SFPD or DA’s office would be unable to share video technology from homeowners or merchants hit by burglars or violent offenders.

We express our strong opposition to this as currently written, and suggest that the Board of Supervisors make the changes recommended by Stop Crime SF before passage of this enabling legislation.

In particular, we suggest:

- 1) Exempting private citizens, non-profits and businesses from the ordinance;
- 2) Exempting the Airport and Port from the ordinance;
- 3) Exempt all investigations for hate crimes, sexual assault, property and violent crimes and terrorism from the ordinance;
- 4) Adding additional time to plan for compliance with the ordinance;
- 5) Adding additional funds for relevant agencies to comply with the ordinance;
- 6) Conducting a cost benefit analysis of technology and the failure to acquire such technology;
- 7) Revising the ordinance after conducting outreach to and dialogue with stakeholders, including crime prevention, anti-crime and victim’s rights groups, as well as business, civil rights and neighborhood groups and law enforcement unions; and
- 8) Include sunset clauses on any ban on technology (e.g., facial recognition tech) after 12 months that may improve in performance over time, to allow time for evaluation of new improvements.

As citizens of San Francisco, we believe that the potential misuse of technology to invade the privacy or abuse the civil liberties of Americans or visitors requires vigilance and policies are warranted. But no ban on cameras or other technologies should be imposed until the policies are first enacted by the Board.

Please let us know if you have any questions by contacting us at: sharp@sharpsf.com.

Sincerely,

S.H.A.R.P. Board of Directors

File # 170110
 Received in committee
 4/15/19
 jm



David Binder Research

California Statewide Survey
Re: Poll Results of Likely 2020 Voters

Topline Findings

A survey of likely November 2020 California voters conducted in March 2019 shows extraordinary support for greater transparency, open debate, and a vote by lawmakers prior to surveillance technology being obtained or used by the government or law enforcement. Bay Area voters strongly support this proposal.

Voters also strongly believe that the government should NOT be using face recognition and similar biometric information, such as your DNA, your voice or the way you walk, to monitor and track individuals. Bay Area voters strongly believe this as well.

On both of these critical questions, there is consistent agreement among Democrats, Republicans and Independents, across voters of all ethnicities and generations, and throughout urban, suburban and rural areas.

The full questions are shown below. Numbers for the Bay Area include the nine Bay Area Counties.

Highlight One:

Three-quarters of voters statewide and in the Bay Area support a law to require public debate and a vote by lawmakers before any surveillance technology is obtained or used by government and law enforcement. Half of voters statewide and in the Bay Area *strongly* support this proposal.

Please tell support or oppose this proposal relating to limiting and requiring oversight for government and law enforcement surveillance.				
<i>Pass a law to require public debate and a vote by lawmakers before any surveillance technology is obtained or used by government and law enforcement.</i>				
	Statewide, Likely voters		Bay Area, Likely Voters	
Support, strongly	50%	→76%	51%	→76%
Support, Somewhat	26		25	
Oppose, Somewhat	9	→19%	7	→17%
Oppose, Strongly	10		10	
Don't know	5		7	

Across the diverse electorate of California, majorities support the proposal to pass a law to require public debate and a vote by lawmakers on these surveillance issues. Particularly in a city like San Francisco with significant racial diversity, the consistency in support for this proposal among all ethnic groups is striking.

<i>Pass a law to require public debate and a vote by lawmakers before any surveillance technology is obtained or used by government and law enforcement.</i>		
Party Affiliation		
	% Support	% Oppose
Democrats	82%	14%
Republicans	64	27
Independents (No Party Preference)	76	19
Age Group		
Millennials and Younger (18-38)	82	17
Generation X (39-54)	76	18
Boomers (55-73)	72	21
Silent Generation (74+)	69	22
Ethnicity		
White	73	22
Latinx	79	15
Asian	72	23
African American* (small sample size)	88	9
Area of Residence		
Urban Area	76	19
Suburb	78	16
Small Town	71	24
Rural Area	77	18

Highlight Two:

82% of likely voters statewide and 79% in the Bay Area disagree with the government being able to monitor and track a person using biometric information. Fewer than 20% of voters statewide and in the Bay Area agree that the government should be using biometric information in this way.

Over 60% of voters statewide and in the Bay Area *strongly* disagree, demonstrating intense opposition to government use of biometric information to monitor and track individuals.

<i>The government should be able to monitor and track who you are and where you go using your biometric information. Do you agree or disagree?</i>				
	Statewide, Likely voters		Bay Area, Likely Voters	
Agree, strongly	5%	→16%	7%	→19%
Agree, Somewhat	11		12	
Disagree, Somewhat	17	→82%	16	→79%
Disagree, Strongly	65		63	
Don't know	2		2	

In a time of heightened partisanship, there is a consensus across political party that the government should not conduct biometric surveillance.

Further, across political parties, ethnic groups, generations, and rural and urban areas of California, there is consistently strong disagreement with the government use of biometric surveillance.

<i>The government should be able to monitor and track who you are and where you go using your biometric information. Do you agree or disagree?</i>		
Party Affiliation		
	% Agree	% Disagree
Democrats	12%	87%
Republicans	21	78
Independents (No Party Preference)	20	79

Age Group		
Millennials and Younger (18-38)	18	81
Generation X (39-54)	16	82
Boomers (55-73)	17	81
Silent Generation (74+)	7	90
Ethnicity		
White	13	85
Latinx	18	80
Asian	27	73
African American* (small sample size)	22	75
Area of Residence		
Urban Area	16	82
Suburb	17	81
Small Town	14	85
Rural Area	16	82

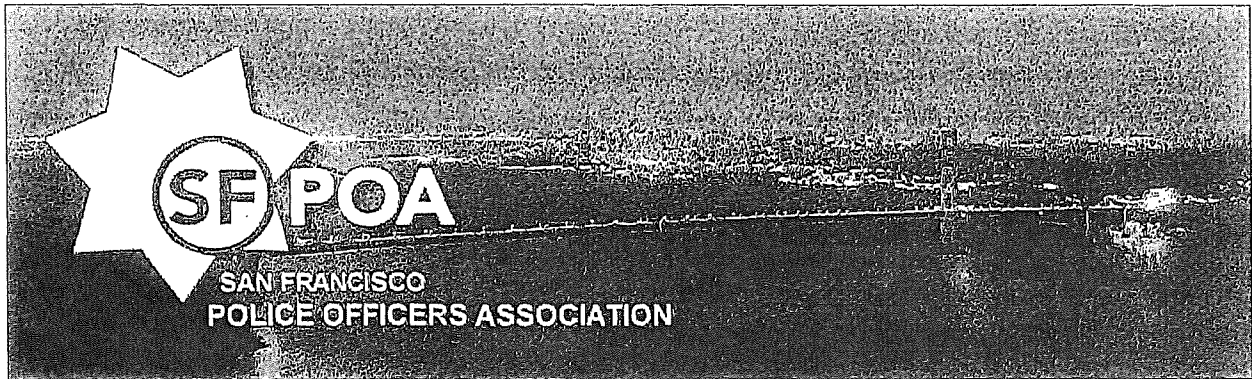
Methodology

David Binder Research conducted a survey of 800 likely November 2020 voters between March 9th and 13th, 2019. Interviews were conducted online, and by cell phone and landline. Latinx respondents were given the choice to take the survey in English or Spanish. The margin of error for the survey is +/- 3.5%, and this survey represents a current snapshot of views on this issue. The margin of error is higher for subgroups of the electorate.



File # 190110
Received in Committee
4/15/19
JW

Fwd: Contact City Hill ASAP on anti-video law
7 messages



Hi everyone -- We need you to send a quick email message ASAP to the San Francisco Board of Supervisors (simple instructions below).

A proposed law to regulate video surveillance will be heard on Monday April 15. It's full of unintended consequences that could make us less safe.

Please express your concern by telling the supervisors to re-think this legislation:

- If you already know enough about this issue and you're ready to act now, [click here for an email template](#) addressed to every supervisor. Adjust the text to your liking and hit send.
- If you want to learn more before sending your message, keep reading below.
- If you wish to appear at the committee hearing in person and speak for one minute during public comment:
 Monday April 15
 10am
 City Hall Room 263
 Third item on [agenda](#)

All the information you need to act is listed below and on [this web page](#). Please share this message with your neighbors.

Thanks for your support,
 Joel Engardio
 Vice President
[Stop Crime SF](#)

BACKGROUND

A proposed law could severely restrict the ability to stop crime with video surveillance. The legislation needs amendments to avoid unintended consequences. The proposed ordinance should also go through a community vetting process before supervisors vote on it. Learn more:

- [San Francisco Chronicle op-ed by Joel Engardio that explains the concerns in simple terms.](#)
- [Open letter from Stop Crime SF that is more technical and offers suggested amendments.](#)

SAMPLE LETTER TO SUPERVISORS

Dear Supervisor,

My name is _____ and I live in the _____ neighborhood. I care deeply about crime in San Francisco. [Note if you or a family member/friend has been a victim of property crime/car break-in/stolen packages/home robbery]

[Stop Crime SF](#), a group of more than 500 San Francisco residents working to reduce and prevent our city's current epidemic of property crime, wrote an [open letter](#) to the Board of Supervisors with concerns about the proposed "Stop Secret Surveillance Ordinance." I share those concerns. The proposed legislation could have unintended consequences that make us less safe by severely curtailing the use of effective traditional video surveillance by burying agencies like the police department in a bureaucratic approval process.

While the essence of this legislation is well-intended, amendments are needed to achieve its goal of protecting privacy while also allowing for the proper use of technology that can keep us safe. Stop Crime SF has offered [reasonable amendments](#) in its open letter.

I am also concerned that this legislation has been rushed with little or no input from the community, public safety agencies and departments that rely on video surveillance like the airport. In other cities where similar technology privacy legislation was drafted and passed, community working groups were formed and a collaborative process crafted a sensible law that worked for everyone. We should do the same in San Francisco.

All stakeholders including homeowners with Nest/Ring video, Next Door community leaders and business owners that have surveillance cameras should be represented. Please allow this public process to happen before voting on the proposed legislation.

Sincerely,
Name
Address

CONTACT YOUR SUPERVISOR

District 1 — Richmond
Sandra Lee Fewer
Sandra.Fewer@sfgov.org

District 2 — Marina
Catherine Stefani
Catherine.Stefani@sfgov.org

District 3 — North Beach, Chinatown
Aaron Peskin
Aaron.Peskin@sfgov.org

District 4 — Sunset
Gordon Mar
Gordon.Mar@sfgov.org

District 5 — Inner Sunset, Cole Valley, Lower Haight, Hayes Valley, Fillmore, Japantown
Vallie Brown
Vallie.Brown@sfgov.org

District 6 — SOMA, Tenderloin
Matt Haney
Matt.Haney@sfgov.org

**District 7 — West of Twin Peaks, West Portal, Inner Sunset, Sunnyside, Lakeshore/Merced
Manor, Westwood Park, Miraloma Park**
Norman Yee
Norman.Yee@sfgov.org

District 8 — Castro, Glen Park
Rafael Mandelman
MandelmanStaff@sfgov.org

District 9 — Mission
Hillary Ronen
Hillary.Ronen@sfgov.org

District 10 — Bayview, Portrero Hill, Visitacion Valley
Shamann Walton
Shamann.Walton@sfgov.org

District 11 — Excelsior
Ahsha Safai
Ahsha.Safai@sfgov.org



April 12, 2019

VIA E-MAIL ONLY

Hon. Norman Yee (President)
Hon. Vallie Brown
Hon. Sandra Lee Fewer
Hon. Matt Haney
Hon. Rafael Mandelman
Hon. Gordon Mar
Hon. Aaron Peskin
Hon. Hillary Ronen
Hon. Ahsha Safai
Hon. Catherine Stefani
Hon. Shamann Walton
San Francisco Board of Supervisors
City Hall, 1 Dr. Carlton B. Goodlett Place
San Francisco, CA
E-Mail: Board.of.Supervisors.@sfgov.org

Re: Acquisition of Surveillance Technology Ordinance (Peskin)

Dear Honorable Board of Supervisors:

I write to urge you to support Supervisor Peskin's Acquisition of Surveillance Technology Ordinance ("Ordinance"), and to share with you my experiences with similar ordinances around the greater Bay Area.

Secure Justice is a 501c (3) advocating against state abuse of power, and for reduction in government and corporate over-reach. We target change in government contracting, and corporate complicity with government policies and practices that are inconsistent with democratic values and principles of human rights.

Surveillance Technology Ordinance

Like other local jurisdictions, Supervisor Peskin has proposed a framework for vetting the potential acquisition or use of surveillance technology. Following the best practices first established in Santa Clara County in 2016, and subsequently enacted into law in Davis, Berkeley, Oakland, Palo Alto, and BART, Supervisor Peskin's proposed Ordinance would require that an impact analysis for each proposed technology acquisition first be performed, and that a proposed use policy be first reviewed, so that the Board can determine whether the benefits of using such technology outweigh the costs (both fiscal, and as to our civil liberties).

I have advocated for all six of the above ordinances, and co-authored four of them, and as Chair of the City of Oakland's Privacy Advisory Commission, I represent to you that the meaningful vetting and deliberation that will occur will lead to greater political buy-in and legitimacy, especially as to the police department's use of surveillance equipment. In addition, the potential impact on civil liberties and misuse of data will be greatly lessened, as experts and members of the public weigh in on the proposed acquisitions and use policies. As a sanctuary city/county, the use and protection of your resident's data should be a heightened concern.¹

Facts as of the date of this letter

- Each of the six existing ordinances follows a similar approval process as the Ordinance. **Each of the six existing ordinances was adopted by unanimous vote of its governing body.**
- Under this model, **no proposal has been permanently rejected** (several have been sent back to staff for additional analysis or draft policy amendments), and **no directive to cease use of existing equipment** has been issued. What we are seeing in practice is that various stakeholders, including the general public and outside subject matter experts, provide feedback to the staff's proposed use policy which usually results in several amendments, before eventual and subsequent unanimous adoption by the governing board.
- As the first entity to adopt this model in the country (June 2016), Santa Clara County has had sufficient time to do a formal review of the ordinance. Only minor amendments were proposed in September 2018 (edits to several headings, and re-arranging several sections for ease of reference). **No amendments to the framework or process were formally proposed by any department. No formal challenges to the governance structure have occurred. No department formally requested relief from compliance.**
- **No disciplinary action has occurred** under this model in the six above jurisdictions pursuant to a complaint from a member of the public (or otherwise, to our knowledge), suggesting that staff is able to comply and that the heightened scrutiny and transparency around both the policy rules and equipment use is ensuring that operators stay within the approved guidelines.
- **No legal actions have commenced** pursuant to the private right of action in the six above jurisdictions, against suggesting that the model is pragmatic.

The above facts demonstrate that this model works in practice, and that compliance is being achieved across the board. It is an elegant solution to complicated questions regarding the use of potentially invasive equipment and our sprint into the age of Big Data, Smart Cities, and proliferation of algorithms making important decisions about our daily lives.

With the passage of your Privacy Principles ballot measure (Prop B), voters in San Francisco recognized that our right to privacy is increasingly impacted with the advance of technology and data mining. The Ordinance provides a mechanism whereby the citizens of San Francisco can

¹ <https://www.mercurynews.com/2018/09/12/bart-staff-ignored-board-to-spy-on-riders-sent-info-ice-could-access/> ("The word sanctuary has lost a lot of its strength," Prieto said. "Trusting any state agency to fully support the undocumented community through sanctuary farces is something we are no longer gambling with." Those lapses of trust, however, are what privacy advocates want to avoid with a surveillance use policy BART's board will consider adopting...")

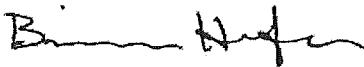
SF Board of Supervisors
Acquisition of Surveillance Technology
April 11, 2019
Page 3 of 3

determine collectively where to draw the lines around the use of surveillance technology and the data collected by it. It is local government at its best.

San Francisco will also benefit from the knowledge and best practices developed by the six jurisdictions that have preceded it. We likely have templates for any existing technology you are using presently, and we routinely provide feedback and templates to any department that asks. I am available to help any San Francisco department achieve compliance with this Ordinance, and I am willing to walk anyone through the Ordinance, and discuss how the process has been working for others.

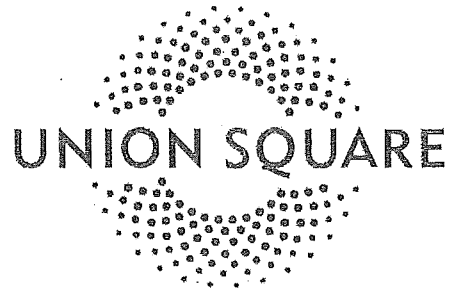
Your leadership and acknowledgment of your constituent's concerns regarding privacy is appreciated. I look forward to San Francisco's talent and sophistication being used to address these important matters of public policy.

Sincerely,



Brian Hofer
Executive Director
(510) 303-2871
brian@secure-justice.org
<https://secure-justice.org/>

cc: Angela Calvillo



April 10, 2019

Board of Supervisors Rules Committee
City Hall
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94102

Dear Supervisors,

On behalf of the Union Square Business Improvement District (USBID) who represents a substantial membership of local employers, employees, property owners, and residents, and provides critical quality of life services for the most visited area of San Francisco, we would like to register our position regarding the proposed Acquisition of Surveillance Technology ordinance that will be appearing before your committee.

We appreciate the sponsor's openness for constructive dialogue throughout this legislative process, as well as the intent of this ordinance to uphold important San Francisco values that protect civil liberties and provide greater transparency in government. As a business community, we also want to bring awareness to the persistent public safety challenges that our members contend with on a daily basis in our city's economic core, and ensure that this ordinance does not place undue administrative burden on the City agencies we work with to deliver vital clean and safe services.

As the crafting of this policy moves forward, we hope for a thoughtful process that brings all stakeholders together, that this legislation seeks to create a single Citywide policy for everyone to follow and takes into consideration all potential use cases, and that it involves the Committee on Information and Technology (COIT) as the City's lead policymaking body for these issues.

We thank you for your continued leadership on these important matters both for our community and for all of San Francisco.

Kind regards,

A handwritten signature in black ink that reads "Karin Flood".

Karin Flood
Executive Director

UNION SQUARE BUSINESS IMPROVEMENT DISTRICT

323 GEARY STREET, SUITE 203 SAN FRANCISCO, CA 94102
TEL (415) 781-7880 FAX (415) 781-0258 VISITUNIONSQUARESF.COM



File # 190110
Received in Committee
4/15/19
for

San Francisco Board of Supervisors
City Hall
1 Dr Carlton B Goodlett Pl.
San Francisco, CA 94102

April 11, 2019

RE: SECURITY CAMERA LEGISLATION

Honorable Members of the Board of Supervisors,

Ahead of the Board of Supervisors Rules Committee hearing on Monday, April 15th, 2019, we would like to register our position on behalf of San Francisco SAFE, Inc. (Safety Awareness for Everyone) and the broader community regarding the recently proposed Acquisition of Surveillance Technology or "Stop Secret Surveillance" ordinance. We would also like to volunteer our expertise to work with the Board and City and County agencies to craft surveillance technology policies that better help promote public safety while protecting civil liberties.

SAFE serves the diverse communities of San Francisco as the go-to non-profit community engagement organization promoting both crime prevention and public safety initiatives for residents, visitors, and local businesses. SAFE works collaboratively across sectors with public and private agencies, including in cooperation with local law enforcement, and seeks to bring community members together through increased awareness and empowerment to improve the quality of life of our neighborhoods.

With decades of experience working as a bridge for residents and the San Francisco Police Department, one of our responsibilities has been to help San Franciscans utilize security cameras as effective crime prevention tools. It is under this mission that we delineate our position for you today. First off, we support the legislative sponsor's intent for upholding important San Francisco values, such as the rights and civil liberties of all people and greater government transparency. Everyone should be included, protected, and welcomed in our city.

As an organization which represents our diverse San Francisco neighborhoods, including many communities of color who have been historically marginalized and impacted by persistent public safety challenges, we also want to make certain that this ordinance does not inhibit the ability of communities to deploy security cameras for their benefit, or place undue administrative burdens that might affect the ability of the City agencies who we work alongside to effectively perform their jobs.

850 Bryant Street
San Francisco
California 94103

Phone:
(415) 673-SAFE
or
(415) 553-1984

Fax:
(415) 553-1967

www.sfsafe.org

*A Community
Crime Prevention
Organization
sponsored in cooperation
with the San Francisco
Police Department*

Attached as Exhibit A are our specific suggested recommendations for potential amendment areas to improve the proposed ordinance. We believe that any policymaking on these issues should bring all stakeholders into the process. We also hope that throughout this process current City functions with respect to these technologies are not diminished during the interim. San Francisco police officers and assistant district attorneys tell us that security cameras are invaluable to arrests and conviction of criminals. This legislation should be tempered so that it protects public safety as well as safeguarding civil liberties.

Furthermore, we would like to see this ordinance establish policies that sets clear standards for all to follow, mitigate any unintended consequences, and considers all potential use cases amongst the various agencies involved. Finally, we strongly urge that this ordinance include the Committee on Information and Technology (COIT), which serves San Francisco as our chief policymaking body for such IT related issues.

In closing, we appreciate your ongoing leadership on behalf of all of San Francisco, and look forward to having a thoughtful dialogue. San Francisco SAFE stands ready to work with the Board and relevant agencies to provide data, information and analysis of their policies at the City's request. Together, we might craft a policy that addresses all concerns, sets the standard, and sustains our position as a beacon of progress for the world.

Thank you,

Daniel Lawson

Daniel Lawson

**President of the Board
San Francisco SAFE, Inc.
(Safety Awareness for Everyone)**

Attachment – Exhibit A: Recommendations

EXHIBIT A

San Francisco SAFE submits the following recommendations for potential revision of the legislation for your consideration:

1. Exclude from the proposed Stop Secret Surveillance Ordinance any public (“open” or “non-secret”) security camera technologies used to enhance crime prevention. Cameras and security devices intended to openly surveil areas to promote the safety and security of any location or facility would not be covered by the Ordinance. These include the following categories:
 - a) Areas/facilities where signage is posted clearly indicating the presence of security cameras and technology. One obvious intent of these security devices is to discourage criminal activity, so the installation is public and open in an attempt to notify potential criminals to refrain from such activity because they are liable to be identified and arrested. This is clearly NOT “secret surveillance.”
 - b) Facilities where surveillance technology is installed to monitor the activity of persons in penal institutions and law enforcement locations where it is clearly understood that activities are under surveillance and privacy is limited. These include facilities in jails, prisons and the entrances to police stations frequented by incarcerated persons, penal authorities and law enforcement officers.
Without this exclusion, the Sheriff’s Department could not monitor operations in the prisons; failure to permit monitoring could result in prisoner abuse or prisoner-on-prisoner violence, or violate federal mandates.
 - c) Surveillance technology mounted on law enforcement vehicles and persons for the purpose of monitoring crimes and interactions between law enforcement officers, suspects and other citizens. Such cameras and technology is crucial for monitoring enforcement and ensuring fair treatment for all and reducing unreasonable racial disparities, as well as for monitoring implementation of police use of force policies, improving law enforcement training and procedures, and documenting criminal conduct. The proposed legislation should specifically define and call out uses that are excluded from the ordinance’s provisions.
The proposed ordinance would require the SFPD to cease use of vehicular or body-mounted cameras during operations within 120 days unless and until both the department and the Board of Supervisors comply with certain requirements; this could result in an increase in unsolved crimes, police misconduct, or misidentification of innocent members of the public.
 - d) Any other areas/facilities where surveillance is open and public, or where surveillance should be reasonably expected to be conducted.
2. Affirmatively approve policies governing use and acquisition of surveillance technology by City agencies, etc., rather than create a blanket prohibition until such policies are adopted by your Board. As written, the proposed ordinance prohibits city departments from using security technology services or equipment until the Board of Supervisors approves a Surveillance Technology policy for the services and equipment. Our analysis of the legislation shows that this cart-before-the-horse approach may significantly limit the ability of law enforcement and prosecutors to fight crime in the meantime, while also reducing the value of San Francisco crime prevention effects.

Surveillance cameras and technology provide valuable photographic, video and other evidence in burglary, robbery and violent crime cases. In particular, video is an important tool to tackle property crime in San Francisco, which has the highest rate of property crime of the nation’s most populated cities.

- a. The Board already has the power to disallow contracts that it would otherwise approve that do not include sufficient civil liberties protections.
 - b. We agree that most City departments should develop clear public policies regarding surveillance technology, but necessary security operations should not cease until the Board can agree on proper policies on a case by case basis. Given the complexity of the issues and the nature of governance, this may take some time.
 - c. These policies might be reviewed by the Board on a case by case basis.
3. Create policy on the use of facial recognition technology and include a sunset clause in any prohibition on the technology. Facial recognition technology is relatively new and imperfect; it is not like DNA technology. Just two years ago, a U.S. General Accounting Office study of facial recognition technology showed a 14 percent failure rate, and the rate was significantly greater when identifying people of color.

Similarly, Chinese-manufactured facial recognition software reportedly had similar trouble properly identifying non-Asians, with higher error rates for other people of color and whites. While facial recognition technology rates are still reportedly better than visual identification by victims or bystanders, the technology should not be the sole factor in arrests. When combined with good police work, however, it can serve as a useful tool.

Facial recognition technology also can help eliminate suspects and result in the release from custody of those unjustly suspected of crimes and avoid placing the burdens of the criminal justice system on other innocent parties.

- a. In this case, we agree with the intent of the legislation and recommend that use of facial recognition technology be prohibited for a determinate period of time (e.g., 180 days) until the SFPD, DA and other appropriate agencies can propose and the Board of Supervisors can adopt a well-crafted public policy.
 - b. An outright ban for a longer period would preclude the possibility of significant technological improvements, just as has occurred in DNA identification in recent years. The facial software has already advanced by leaps and bounds in recent years, and much better accuracy may already be available or be around the corner. Refinements that address today's shortcomings could make facial recognition a valuable security tool.
 - c. Even if facial recognition has not advanced significantly, a well-crafted public policy can prevent racial disparities and ensure this is only one tool in a toolbox that is necessarily not completely perfect.
4. Consider other suggested amendments including:
- **Exclude SFO and the Port of San Francisco from certain requirements of this ordinance.**
Airports and ports serve as the gateway to San Francisco and are particularly vulnerable to certain types of terrorist activity, and public safety and federal and international requirements demand different standards.
 - **Change the effective date of the Ordinance to the beginning of the next fiscal year, or 180 days after enactment, whichever comes later.**
Some departments do not have the expertise or resources to fulfil the detailed and highly technical requirements of this proposed legislation without additional time. Meeting the requirements of the ordinance might unduly interfere with critical day-to-day operations.

- **Require that additional funds to comply with the requirements of this ordinance be explicitly allocated to each affected department in the applicable fiscal year.**
Reducing existing services in order to comply with the proposed ordinance's requirements is unacceptable.
- **Revise compliance dates.**
In Sec. 19.B.5 (a) to 180 days and in Sec. 19.B.5 (b) to 150 days, for reasons stated above.
- **Require any cost benefit analysis to include an estimate of economic and social costs to the public as well as city government if the ability to utilize surveillance technology is obstructed.** Any cost benefit analysis should also examine the cost of alternatives to surveillance technology as well.
- **Consider deleting requirements for public release of identification of certain locations for surveillance technology in selected instances.**
Technology owned by private owners should not be subject to identification of locations. This information should be classified for selected confidential/secret locations to protect against criminal activity or terrorist activities. There is no reason to give potential lawbreakers a roadmap to areas where they can safely carry out criminal activities. (This does not apply to public or open locations for surveillance cameras where signage is present.)
- **Consider the public safety impacts of reduced surveillance at large crowd events such as the Pride Parade, large outdoor concerts and street fairs, and the Chinese Lunar New Year celebration.**
These events might become targets for hate-group terrorists if it became known that surveillance technology use was reduced at such occasions.
- **Allow the public to provide surveillance evidence to City agencies for use in crime investigations.**

Private citizens in their homes and businesses should be exempt from the requirements of this ordinance. The proposed law doesn't restrict a private citizen from installing a camera in her home. But the ordinance would seemingly require the city to develop a use policy and receive Board of Supervisors approval before "entering into agreement with a non-city entity to acquire, share, or otherwise use surveillance technology." Private citizens and businesses should be able to provide video footage and photos to the SFPD or DA without restriction in the event of a suspected crime, and these agencies should be allowed to use these products/information.



April 9, 2019

Mayor London Breed
 Supervisor Norman Yee
 Supervisor Sandra Lee Fewer
 Supervisor Catherine Stefani
 Supervisor Aaron Peskin
 Supervisor Gordon Mar
 Supervisor Vallie Brown
 Supervisor Matt Haney
 Supervisor Rafael Mandelman
 Supervisor Hillary Ronen
 Supervisor Shamann Walton
 Supervisor Ahsha Safai
 San Francisco Board of Supervisors
 City Hall, 1 Dr. Carlton B. Goodlett Place
 San Francisco, California

Re: SUPPORT for the Stop Secret Surveillance Ordinance

Dear Supervisors,

We are a coalition of civil rights organizations writing to express support for the Stop Secret Surveillance Ordinance being considered at the April 15, 2019 meeting of the Rules Committee. This legislation will improve public safety with a straightforward and open process for considering surveillance technology proposals, safeguard against dangerous and biased surveillance practices, and provide the public and Board with a necessary voice in important surveillance decisions affecting the City. We urge you to support this ordinance.

This letter explains the purpose of the Ordinance and how it helps protect the privacy and safety of all San Francisco residents. First, the letter outlines the problems addressed by the Ordinance. Second, the letter explains why the City should prevent the deployment of face surveillance technology that poses a threat to people in San Francisco, regardless of its accuracy. Finally, the letter encourages the Board to ensure that the Sheriff and District Attorney are fully subject to the Ordinance.

1. The Ordinance Ensures Diverse Community Members Are Part of Important Public Safety Decisions

Surveillance technologies such as automated license plate readers, drones, sensor-equipped streetlights, and predictive policing software can collect sensitive personal information about where people go, who they associate with, and even how they feel. All too often, such systems operate out of public view and collect information without the knowledge or consent of residents. When used by public agencies, surveillance technology can fundamentally change the relationship between governments and residents, influencing decisions about who receives a government service, who is monitored and subjected to potentially dangerous encounters with the police, and whether people feel comfortable organizing and engaging in activism. San Francisco should not deploy surveillance technology on its residents without public debate about how these technologies work and their potential harms, and clear guidelines for how the technology can be used.

Public and Board scrutiny of surveillance technology is essential because the impacts of surveillance technology are not equitably distributed – time and again, data collection and processing systems focus their digital gaze on immigrants, people of color, and the poor. As a result, actions taken using this data and errors resulting from flawed data or operator misuse disproportionately impact and potentially harm these communities as well. Without adequate public debate or safeguards to prevent misuse, surveillance technology will harm community members. We know this because it has already happened in San Francisco and the Bay Area.

Many Bay Area police departments have secretly deployed surveillance system without policies to govern their use, provide accountability, and ensure people's safety. This has put immigrant and Black community members in harm's way. Here in San Francisco, SFPD officers held a Black woman at gunpoint outside her car after misusing an automated license plate reader that they operated without an adequate policy to prevent potentially grave mistakes.¹ According to a 2015 report, Oakland police's use of license plate readers was effectively concentrated in low-income and Black communities, perpetuating a long history of over-policing.² In San Jose, police

¹ Kade Crockford, *San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error*, ACLU, May 13, 2014, <https://www.aclu.org/blog/privacy-technology/location-tracking/san-francisco-woman-pulled-out-car-gunpoint-because>.

² Dave Maass, *What You Can Learn From Oakland's Raw ALPR Data*, Electronic Frontier Foundation, Jan. 21, 2015, <https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data>.

secretly purchased a drone without meaningfully consulting Muslim community members and other residents who have been targeted by the government for their religious affiliation.³ And in Fresno, the police department used social media surveillance software from a vendor that actively encouraged police to spy on Black Lives Matter activists.⁴

Information about residents in local surveillance systems is also vulnerable to demands by federal agencies such as ICE, who may seek to exploit it to fuel inhumane policies. This is not a hypothetical threat – we recently learned that Immigration and Customs Enforcement has purchased access to a driver location database to which police departments can contribute locally-collected data.⁵ We know that ICE can use that database to assist its efforts to locate and deport community members. The potential vulnerability of local surveillance databases to potential access by agencies such as ICE could threaten San Francisco’s commitment to be a sanctuary city for all residents. This Ordinance would require proposals for such systems to be subject to Board and public scrutiny so that residents are not harmed.

The secretive and unaccountable use of surveillance technology not only harms residents, it damages community trust in local governments.⁶ Other cities have experienced this first hand, such as when Oakland’s City Council faced a public backlash after the public learned about secret plans to build a DHS-funded “Domain Awareness Center” that aggregated surveillance feeds from around the city.⁷ Likewise, when citizens and the Seattle City Council discovered that the police department had acquired drones three years earlier, the ensuing protests led the Mayor to shelve the program, stating that Seattle needed to focus on “community building.”⁸ In both cases, the absence of public debate and a process for elected leaders to evaluate technologies triggered an avoidable public controversy that bred distrust in government and sapped staff time and taxpayer resources.

2. The Ordinance Ensures Democratic Debate and Oversight for Surveillance Technology Decisions

This proposed Ordinance is straightforward and ensures proper democratic debate, transparency, and oversight of surveillance technologies. The Ordinance requires that a city department seeking surveillance technology explain to the public how it works and draft clearly written rules for that specific technology that are designed to protect the public. The Ordinance also requires that the proposal be heard by the Board of Supervisors at a regular public meeting. If the Board approves a new surveillance technology at that meeting, the Ordinance ensures the Board and public will be able to understand and evaluate how it is used through the creation of a simple

³ Thomas Mann Miller, *San Jose Police Department's Secret Drone Purchase: Where's the Accountability?*, ACLU-NorCal, July 30, 2014, <https://www.aclunc.org/blog/san-jose-police-departments-secret-drone-purchase-wheres-accountability>.

⁴ Justin Jouvenal, *The new way police are surveillance you: calculating your threat 'score*, Wash. Post, Jan. 10, 2016, https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.3514f883ceeb.

⁵ Vasudha Talla, *Documents Reveal ICE Using Driver Location Data from Local Police for Deportations*, ACLU.org, Mar. 13, 2019, <https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data>.

⁶ A 2014 ACLU of California survey found that at least 90 California communities were in possession of various surveillance technologies, and that public debate rarely occurred when technologies were proposed. *State of Surveillance in California – Findings & Recommendations*, January 2015, https://www.aclunc.org/sites/default/files/201501-aclu_ca_surveillancetech_summary_and_recommendations.pdf.

⁷ Brian Wheeler, *Police Surveillance: The US city that beat Big Brother*, Sept. 29, 2016, <http://www.bbc.com/news/magazine-37411250>.

⁸ *Seattle Mayor ends police drone efforts*, USA Today, Feb. 7, 2013, <https://www.usatoday.com/story/news/nation/2013/02/07/seattle-police-drone-efforts/1900785/>.

Annual Report. The Ordinance also ensures that there are written safety measures for existing surveillance technologies already in use.

The Ordinance appropriately requires that the public and democratically-elected Board play a role in evaluating new surveillance technologies before they are acquired or used. And by requiring straightforward safeguards and an annual report, the Ordinance helps ensure community members are not harmed and that the Board fully understands how approved technologies are used. This has produced better outcomes in other Northern California communities with similar laws. Since 2016, Santa Clara County, Oakland, Berkeley, Davis, Palo Alto, and BART have all passed similar ordinances to the one before the Board. On repeated occasions, these communities have come to better decisions about surveillance technology – whether it was Santa Clara’s imposition of safeguards on body cameras or Oakland’s scrutiny of a relationship with a federal “fusion center” – because of the process put in place by their local surveillance ordinance. We urge San Francisco to adopt the same common-sense process for considering new surveillance.

3. The Ordinance Protects San Franciscans from Dangerous and Biased Face Surveillance

We also fully endorse the Ordinance’s prohibition on the use of facial recognition technology by city departments. This is a technology that poses a threat to people of color and would supercharge biased government surveillance of our communities. The use of this technology by government agencies poses a unique threat to public safety and the well-being of people in San Francisco, regardless of the technology’s accuracy. San Francisco should refuse to allow government agencies to acquire or use it for at least three reasons: first, due to flaws in face surveillance systems; second, because such systems are frequently built upon biased datasets; and finally, because face surveillance would supercharge invasive and discriminatory government surveillance, regardless of its accuracy.

The biased algorithms and processes that power face surveillance technology pose a threat to people of color. Multiple tests of this technology indicate it is less accurate for darker-skinned people. Peer-reviewed academic research by researchers at MIT has demonstrated that prominent facial recognition technology products perform more poorly for people with darker skin and women.⁹ Last year, Amazon’s Rekognition face surveillance product misidentified 28 members of Congress as persons in a database of booking photos in a test conducted by the ACLU of Northern California.¹⁰ Of those false matches, 39 percent were people of color, even though people of color only constitute 19 percent of Congress. In practice, an erroneous face surveillance system could misinform and influence a government employee’s decision about how to approach a person, including the decision of whether to use force. These kind of flawed systems should not be used to make decisions about San Franciscans’ lives.

The databases the underlie facial recognition systems are frequently biased as well. Facial recognition systems are commonly connected to databases of mugshot photos. These photos are

⁹ Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81: 1-15, 2018, <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Natasha Singer, *Amazon Is Pushing Facial Technology That a Study Says Could Be Biased*, New York Times, Jan 24, 2019, <https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html>.

¹⁰ Jacob Snow, *Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU Free Future Blog, July 26, 2018, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>.

then used as a reference point when the system searches for people in the world. But because mugshot databases reflect historical over-policing of communities of color, facial recognition “matching” databases are likely disproportionately made up of people of color. If such systems are connected to officer body cameras or surveillance cameras, these communities may be unfairly targeted simply because they appeared in another database or were subject to discriminatory policing in the past.

Face surveillance will also fuel invasive and discriminatory government surveillance. People should be free to go about their daily lives without the government knowing whether they visit a bar or an abortion clinic, march at a political rally, or attend a religious service. Yet with the flip of a switch, the City could add face surveillance to public CCTV cameras, sensor-equipped smart street lights, or even officer-worn body cameras, creating a citywide surveillance network that could track and recognize residents as they move across town. Face surveillance technology makes it easy for the government to track and store intimate details from our private lives, all with little to no human effort. And like the surveillance systems that came before, the harms will fall hardest on people of color, religious minorities, and immigrants. At a time when public protest is at an all-time high and the federal government is attacking immigrants and activists, San Francisco should refuse to build face surveillance systems that could easily be misused for dangerous, authoritarian surveillance.

Face surveillance will not make the San Francisco community safer and could lead to grave harm. It would chill civil engagement and subject residents and visitors to continuous monitoring and potentially violent contacts with law enforcement if it produces erroneous results. Regardless of accuracy, systems built on face surveillance will amplify and exacerbate historical and existing biases that harm immigrants, religious minorities, activists, and people of color. An identification—whether accurate or not—could cost people their freedom or even lives. San Francisco should refuse to go down this road.

4. The Sheriff and District Attorney Should Be Fully Subject to Democratic Oversight and Not Allowed to Unilaterally Exempt Themselves from the Ordinance

It is essential that the Ordinance protect community members regardless of which City Department possesses or operates the surveillance technology. As written, the Ordinance covers all city officials, departments, boards, commissions, including but not limited to the police department, sheriff’s office, and district attorney. But we are concerned about two provisions in the current draft Ordinance that allow the District Attorney or Sheriff to unilaterally exempt themselves from democratic oversight under the Ordinance by declaring that they are acting in a prosecutorial or investigatory capacity.¹¹ These provisions impose an unacceptable veil of secrecy, both as a matter of public policy, and because they undermine the Board’s supervisory authority under state law.

The Board of Supervisors has an obligation to exercise supervision of the conduct of local departments and officers, including the Sheriff and the District Attorney.¹² Last year the

¹¹ This provision appears in the definition of “City Department” at Chap. 19B1 and at Sec. 19B.2.

¹² By law, the Board possess substantial authority to supervise district attorneys and sheriffs, allocate their budgets, approve county contracts, manage grant funding, request reports, and set rules for the acquisition and use of county property. *See, e.g.*, Cal. Govt. Code. § 25303 (mandating that the Board “shall see that [county officers] faithfully perform their duties...and when necessary, require them to...make reports and present their books and accounts for inspection”); Cal. Govt. Code § 23004(c) (authorizing the Board to enter into contracts on behalf of the county); Cal. Govt. Code § 53701 (authoring the Board to accept grants or loans made available by the federal government to finance public works); Cal. Govt. Code § 54202 (declaring that local agencies may adopt policies and procedures governing purchases of supplies and equipment used by the local agency);

California Senate Judiciary Committee specifically recognized the power of Boards of Supervisors to “supervise the official conduct of sheriffs and district attorneys, especially in connection with their management, or disbursement of public funds to procure surveillance technologies.”¹³ The Surveillance Ordinance applies these authorities to the acquisition, use, and oversight of various surveillance technologies.

We urge San Francisco to ensure the District Attorney and Sheriff are fully covered by the Ordinance’s requirements.¹⁴ At a minimum, the Ordinance should mandate that the public and Board be informed and given the opportunity to discuss any efforts by the District Attorney and Sheriff to exempt themselves from the Ordinance.

5. Conclusion

Thank you for your consideration of this essential Ordinance designed to protect public safety and ensure that the Board and community have a voice in decisions about surveillance technology in San Francisco. We look forward to working with the Board to pass and implement this Ordinance. Please let us know if you have any questions.

Sincerely,

ACLU of Northern California
Asian Americans Advancing Justice – Asian Law Caucus
Asian Law Alliance
Centro Legal de la Raza
Coalition on Homelessness
Council on American-Islamic Relations SF-Bay Area
Color of Change
Data for Black Lives
Electronic Frontier Foundation
Faith in Action Bay Area
Freedom of the Press Foundation
Greenlining Institute
Harvey Milk LGBTQ Democratic Club
Indivisible SF
Justice 4 Mario Woods Coalition
National Center on Lesbian Rights
Media Alliance
Lawyers’ Committee for Civil Rights
Oakland Privacy
San Francisco Democratic Socialists of America
San Francisco Public Defender Racial Justice Committee
Secure Justice
SF Latino Democratic Club
Tenth Amendment Center
Transgender Law Center

¹³ California Senate Judiciary Committee Analysis of SB 1186 (emphasis added; quotations omitted), available here: https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB1186#.

¹⁴A similar ordinance in Santa Clara County accomplishes that by requiring that the Board or a court of law – and not simply the Sheriff or DA acting unilaterally – make a determination that oversight under the ordinance obstructs a sheriff or DA’s prosecutorial or investigatory functions. Santa Clara County Ordinance Code Sec. A40-5, https://library.municode.com/ca/santa_clara_county/codes/code_of_ordinances?nodeId=TITAGEAD_DIVA40SUECCOAF_SA40-5COEXSUTE.



March 27, 2019

President Norman Yee
Supervisor Sandra Lee Fewer
Supervisor Catherine Stefani
Supervisor Aaron Peskin
Supervisor Gordon Mar
Supervisor Vallie Brown
Supervisor Matt Haney
Supervisor Rafael Mandelman
Supervisor Hillary Ronen
Supervisor Shamann Walton
Supervisor Ahsha Safai

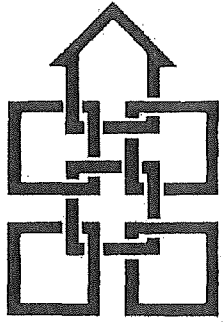
Dear Board of Supervisors:

I am writing to you on behalf of Color Of Change, the nation's largest online racial justice organization, with more than 1.6 million members nationally and nearly 50,000 members located in the Bay area. We urge you to adopt the Stop Secret Surveillance Ordinance, which is up for consideration at the April 15, 2019 meeting of the Rules Committee, and proposes restrictions on the use of surveillance technologies and recommends banning the use of harmful and discriminatory surveillance technologies in San Francisco.

Time and time again, surveillance technologies have been used to target Black communities, immigrants, poor people, religious minorities, and communities of color.¹ When employed by police departments and governments, technologies like automated license plate readers, camera-equipped drones, stingrays, and predictive policing software increase the number of unnecessary interactions between marginalized communities and the police, and threaten San Franciscans' safety. Incidents like that of a Black woman being held at gunpoint outside her car as a result of the San Francisco Police Department's misuse of an automated license plate

¹ "The new way police are surveilling you: calculating your threat 'score,'" Washington Post, 10 January 2016,

https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.3514f883cee



COALITION ON
HOMELESSNESS
san francisco

March 20, 2019

Dear Elected Official,

The Coalition on Homelessness is writing to request that you support Supervisor Aaron Peskin's "Stop Secret Surveillance" Ordinance that would require San Francisco City Departments to adopt a Surveillance Data Policy if they intend to use, continue to use, or acquire surveillance technology equipment. The legislation would also require any agency wishing to use such technology to get approval from the San Francisco Board of Supervisors, as well as provide an annual audit of such technology use. Finally, the legislation categorically prohibits the use of any Facial Recognition Technology by any San Francisco city departments.

This legislation is urgently needed given the slew of new surveillance technologies now available and the dearth of regulation on the topic. This legislation would be one of the first in the nation to ban Facial Recognition Technology and would join San Francisco with Santa Clara and a few other California counties in regulating surveillance technology.

Story after story in the media show the ways in which such technologies have either deliberately or inadvertently targeted people of color, violated the citizenry's civil liberties, and laid the groundwork for a truly Orwellian society where people's every move is monitored and potentially criminalized.

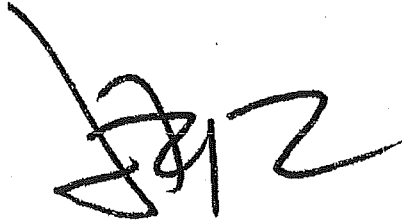
While arguments can, and have, been made about the benefits of surveillance technology to protect public safety, we strongly believe such technologies need to be regulated, and in the case of Facial Recognition technology, prohibited. There is no place in the City and County of San Francisco for the use of such technology. In its current iteration the technology is inaccurate and tends to single out communities of color. But even were the technology "accurate" and did not directly target people of color, the very nature of the technology tends to focus on the poorest and most disenfranchised communities in the city given the current social and economic structure of American society. For example, shelter residents since 2004 have been required to submit to biometric imaging of their face in order to qualify for 90 day shelter beds. This practice immediately led to many undocumented residents becoming fearful of the use of this technology to find and deport them, and the shelters saw a decrease in use by undocumented individuals.

For this reason, we support a complete ban of the use of Facial Recognition Technology in San Francisco. Given the march of technology there will doubtless be attempts to introduce Facial Recognition Technology. (This piece of legislation deals with that eventuality by creating a stringent

process that any attempt to introduce Facial Recognition Technology will have to navigate.)

We appreciate your interest in this important privacy and civil liberties matter. We feel confident you would be willing to help get such legislation passed.

Sincerely,

A handwritten signature in black ink, appearing to read 'JF', written over a horizontal line.

Jennifer Friedenbach
Executive Director

468 Turk St.
San Francisco, CA 94102
415.346.3740 TEL

468 Turk St.
San Francisco, CA 94102
415.346.3740 TEL
415.775.5639 FAX
www.cohsf.org



NATIONAL CENTER FOR LESBIAN RIGHTS

NATIONAL OFFICE
870 Market St Suite 370
San Francisco CA 94102
tel 415 392 6257
fax 415 392 8442
info@nclrights.org
www.nclrights.org

March 6, 2019

Supervisor Aaron Peskin
City Hall
1 Dr. Carlton B. Goodlett Place, Room 244
San Francisco, CA 94102-4689

RE: Stop Secret Surveillance Ordinance – Support

Dear Supervisor Peskin,

The National Center for Lesbian Rights (NCLR) strongly supports the Stop Secret Surveillance Ordinance. This ordinance would require the City and County of San Francisco to adopt a Surveillance Data Policy if they intend to use, continue to use, or acquire surveillance technology equipment. The ordinance would also require any agency wishing to use surveillance technology to get approval from the San Francisco Board of Supervisors and provide an annual audit of the agency's use of that technology. Finally, the ordinance expressly prohibits the use of any facial-recognition technology by any department or agency of the City and County of San Francisco.

NCLR is a national legal organization committed to advancing the civil and human rights of lesbian, gay, bisexual, and transgender people and their families through litigation, legislation, policy, and public education. Discrimination and harassment by law enforcement is an ongoing and pervasive problem for LGBT individuals, particularly those who are members of low-income communities or communities of color.¹ Because surveillance efforts have historically targeted marginalized and vulnerable communities, NCLR strongly believes surveillance technologies need to be regulated, and in the case of facial-recognition technology, prohibited.

There is no place in the City and County of San Francisco for the use of facial-recognition technology. In its current iteration, the technology is inaccurate and tends to deliberately or inadvertently target people of color and other vulnerable communities. The inaccuracies and biases built into facial-recognition technology also amplify the significant concerns that this technology will deprive individuals of key constitutional safeguards that undergird our criminal justice system.

¹ See Williams Institute, *Discrimination and Harassment by Law Enforcement Officers in the LGBT Community* (2015), <https://williamsinstitute.law.ucla.edu/wp-content/uploads/LGBT-Discrimination-and-Harassment-in-Law-Enforcement-March-2015.pdf>.



NATIONAL CENTER FOR LESBIAN RIGHTS

This ordinance is urgently needed given the onslaught of new surveillance technologies now available and the lack of regulation on the topic. By taking this important step, the City and County of San Francisco would be leading the nation as one of the first jurisdictions to ban facial-recognition technology and would join Santa Clara and other counties in California that are already regulating the use of surveillance technology. For these reasons, NCLR strongly supports the Stop Secret Surveillance Ordinance.

Sincerely,

A handwritten signature in black ink, appearing to read "Cindy L. Myers". The signature is fluid and cursive, with a long horizontal stroke at the end.

Cindy L. Myers, Ph.D.
Interim Executive Director
National Center for Lesbian Rights

BOARD of SUPERVISORS



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

MEMORANDUM

TO: Linda Gerull, Executive Director/CIO
Department of Technology

FROM: Victor Young, Assistant Clerk *vy*
Rules Committee

DATE: February 6, 2019

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee has received the following proposed legislation, introduced by Mayor Breed on January 29, 2019:

File No. 190110

Ordinance amending the Administrative Code to require that City departments acquiring Surveillance Technology submit a Board of Supervisors approved Surveillance Technology Policy Ordinance and a Surveillance Impact Report to the Board in connection with any request to appropriate funds for the purchase of such technology or to accept and expend grant funds for such purpose, or otherwise to procure Surveillance Technology equipment or services; require each City department that owns and operates existing surveillance technology equipment or services to submit to the Board a proposed Surveillance Technology Policy Ordinance governing the use of the surveillance technology; and requiring the Controller, as City Services Auditor, to audit annually the use of surveillance technology equipment or services and the conformity of such use with an approved Surveillance Technology Policy Ordinance and provide an audit report to the Board of Supervisors.

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.

BOARD of SUPERVISORS



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

MEMORANDUM

TO: Kanishka Karunaratne Cheng, Mayor's Office,
Liaison to the Board of Supervisors
Ben Rosenfield, Controller, Office of the Controller
George Gascon, District Attorney, Office of the District Attorney
Vickie Hennessy, Sheriff, Sheriff's Department

FROM: Victor Young, Assistant Clerk
Rules Committee

DATE: March 19, 2019

SUBJECT: LEGISLATION INTRODUCED

The Board of Supervisors' Rules Committee has received the following proposed legislation, introduced on January 29, 2019:

File No. 190110

Ordinance amending the Administrative Code to require that City departments acquiring Surveillance Technology submit a Board of Supervisors approved Surveillance Technology Policy Ordinance and a Surveillance Impact Report to the Board in connection with any request to appropriate funds for the purchase of such technology or to accept and expend grant funds for such purpose, or otherwise to procure Surveillance Technology equipment or services; require each City department that owns and operates existing surveillance technology equipment or services to submit to the Board a proposed Surveillance Technology Policy Ordinance governing the use of the surveillance technology; and requiring the Controller, as City Services Auditor, to audit annually the use of surveillance technology equipment or services and the conformity of such use with an approved Surveillance Technology Policy Ordinance and provide an audit report to the Board of Supervisors.

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.

c: Mawuli Tugbenyoh, Mayor's Office
Rebecca Peacock, Mayor's Office
Andres Power, Mayor's Office
Toddy Rydstrom, Office of the Controller
Tonia Lediju, Office of the Controller
Cristine Soto DeBerry, Office of the District Attorney
Maxwell Szabo, Office of the District Attorney
Johanna Saenz, Sheriff's Department
Katherine Johnson, Sheriff's Department
Nancy Crowley, Sheriff's Department

Introduction Form

By a Member of the Board of Supervisors or Mayor

BOARD OF SUPERVISORS
SAN FRANCISCO

2019 JAN 29

Time stamp
or meeting date

I hereby submit the following item for introduction (select only one):

BY _____

- 1. For reference to Committee. (An Ordinance, Resolution, Motion or Charter Amendment).
- 2. Request for next printed agenda Without Reference to Committee.
- 3. Request for hearing on a subject matter at Committee.
- 4. Request for letter beginning : "Supervisor [] inquiries"
- 5. City Attorney Request.
- 6. Call File No. [] from Committee.
- 7. Budget Analyst request (attached written motion).
- 8. Substitute Legislation File No. []
- 9. Reactivate File No. []
- 10. Topic submitted for Mayoral Appearance before the BOS on []

Please check the appropriate boxes. The proposed legislation should be forwarded to the following:

- Small Business Commission
- Youth Commission
- Ethics Commission
- Planning Commission
- Building Inspection Commission

Note: For the Imperative Agenda (a resolution not on the printed agenda), use the Imperative Form.

Sponsor(s):

Peskin; Yee

Subject:

[Administrative Code - Acquisition of Surveillance Technology]

The text is listed:

Ordinance amending the Administrative Code to require that City departments acquiring Surveillance Technology submit a Board of Supervisors approved Surveillance Technology Policy ordinance and a Surveillance Impact Report to the Board in connection with any request to appropriate funds for the purchase of such technology or to accept and expend grant funds for such purpose, or otherwise to procure Surveillance Technology equipment or services; require each City department that owns and operates existing surveillance technology equipment or services to submit to the Board a proposed Surveillance Technology Policy ordinance governing the use of the surveillance technology; and requiring the Controller, as City Services Auditor, to audit annually the use of surveillance technology equipment or services and the conformity of such use with an approved Surveillance Technology Policy ordinance and provide an audit report to the Board of Supervisors.

Signature of Sponsoring Supervisor: [Signature]