

File No. 190110

Committee Item No. 3

Board Item No. _____

COMMITTEE/BOARD OF SUPERVISORS

AGENDA PACKET CONTENTS LIST

Committee: Rules Committee

Date April 15, 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"/>	
<input type="checkbox"/>	<input type="checkbox"/>	

Completed by: Victor Young Date April 11, 2019

Completed by: _____ Date _____

[Administrative Code - Acquisition of Surveillance Technology]

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.

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

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

Section 1. General Findings.

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

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

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

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

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

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

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

23 ///

24 ///

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 summary of all requests for Board of Supervisors' approval for a Surveillance
5 Technology Policy ordinance.

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

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

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

14 (1) The District Attorney or Sheriff certifies in writing to the Controller that acquisition
15 of Surveillance Technology is necessary to perform an investigative or prosecutorial function, and

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

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

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

24 "Surveillance Impact Report" means a written report that includes at a minimum the following:
25

- 1 (1) Information describing the Surveillance Technology and how it works, including
2 product descriptions from manufacturers;
- 3 (2) Information on the proposed purpose(s) for the Surveillance Technology;
- 4 (3) If applicable, the general location(s) it may be deployed and crime statistics for any
5 location(s);
- 6 (4) An assessment identifying any potential impact on civil liberties and civil rights and
7 discussing any plans to safeguard the rights of the public;
- 8 (5) The fiscal costs for the Surveillance Technology, including initial purchase,
9 personnel and other ongoing costs, and any current or potential sources of funding;
- 10 (6) Whether use or maintenance of the technology will require data gathered by the
11 technology to be handled or stored by a third-party vendor on an ongoing basis; and
- 12 (7) A summary of the experience, if any, other governmental entities have had with the
13 proposed technology, including information about its effectiveness and any known adverse information
14 about the technology such as unanticipated costs, failures, or civil rights and civil liberties abuses.
- 15 “Personal communication device” means a cellular telephone that has not been modified
16 beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or
17 similar wireless two-way communications and/or portable Internet accessing devices, whether
18 procured or subsidized by a City entity or personally owned, that is used in the regular course of
19 conducting City business.
- 20 “Surveillance Technology” means any software, electronic device, system utilizing an
21 electronic device, or similar device used, designed, or primarily intended to collect, retain, process, or
22 share audio, electronic, visual, location, thermal, biometric, olfactory or similar information
23 specifically associated with, or capable of being associated with, any individual or group. Surveillance
24 Technology” includes but is not limited to the following: international mobile subscriber identity
25 (IMSI) catchers and other cell site simulators; automatic license plate readers; electric toll readers;

1 closed-circuit television cameras; gunshot detection hardware and services; video and audio
2 monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and
3 wearable body cameras; mobile DNA capture technology; biometric software or technology, including
4 facial, voice, iris, and gait-recognition software and databases; software designed to monitor social
5 media services; x-ray vans; software designed to forecast criminal activity or criminality; radio-
6 frequency I.D. (RFID) scanners; and tools, including software and hardware, used to gain
7 unauthorized access to a computer, computer service, or computer network. Surveillance Technology
8 does not include the following devices, hardware, or software:

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

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

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

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

20 (5) Physical access control systems, employee identification management systems, and
21 other physical control systems;

22 (6) Infrastructure and mechanical control systems, including those that control or
23 manage street lights, traffic lights, electrical, natural gas, or water or sewer functions;
24
25

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

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

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

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

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

14 (12) Parking Ticket Devices;

15 (13) Police Department interview rooms, holding cells, and internal security
16 audio/video recording systems;

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

20 (15) Police department early warning systems; and

21 (16) Computers, software, hardware, or devices used to monitor the safety and security
22 of City facilities and their occupants.

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

24 (1) A description of the product and services addressed by the Surveillance Technology,
25 including manufacturer and model numbers and/or the identity of any provider(s) whose services are

1 essential to the functioning or effectiveness of the Surveillance Technology equipment or services for
2 the intended purpose;

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

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

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

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

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

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

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

23 (9) Which governmental agencies, departments, bureaus, divisions, or units that may
24 receive data collected by the Surveillance Technology operated by the Department, including any
25

1 required justification or legal standard necessary to share that data and how it will ensure that any
2 entity receiving such data complies with the Surveillance Technology Policy;

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

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

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

14
15 **SEC. 19B.2. BOARD OF SUPERVISORS APPROVAL OF SURVEILLANCE**
16 **TECHNOLOGY POLICY.**

17 (a) Except as stated in subsection (c), a Department must obtain Board of Supervisors approval
18 by ordinance of a Surveillance Technology Policy under which the Department will acquire and use
19 Surveillance Technology, prior to engaging in any of the following:

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

22 (2) Acquiring or borrowing new Surveillance Technology, including but not limited to
23 acquiring Surveillance Technology without the exchange of monies or other consideration;
24
25

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

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

6 (b) Notwithstanding the provisions of this Chapter 19B, it shall be unlawful for any Department
7 to obtain, retain, access, or use: 1) any Face Recognition Technology; or 2) any information obtained
8 from Face Recognition Technology.

9 (c) If either the District Attorney or Sheriff certifies in writing to the Controller that acquisition
10 of Surveillance Technology is necessary to perform an investigative or prosecutorial function and
11 provides in writing to the Controller either an explanation of how compliance with this Chapter 19B
12 will obstruct their investigative or prosecutorial function or a declaration that the explanation itself
13 will obstruct either function, the District Attorney or Sheriff shall simultaneously submit a copy of the
14 document to the Clerk of the Board of Supervisors so that the Board in its discretion may hold a
15 hearing and request that the District Attorney or Sheriff appear to respond to the Board's questions
16 regarding such certification, explanation, and/or declaration.

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

20
21 **SEC. 19B.3. SURVEILLANCE IMPACT REPORT AND SURVEILLANCE TECHNOLOGY**
22 **POLICY SUBMISSION.**

23 (a) The Department seeking approval under Section 19B.2 shall submit to the Board of
24 Supervisors and publicly post on the Department website a Surveillance Impact Report and a proposed
25

1 Surveillance Technology Policy ordinance at least 30 days prior to the public meeting where the Board
2 will consider that Surveillance Technology Policy ordinance pursuant to Section 19B.2.

3 (b) Prior to submitting the Surveillance Technology Policy ordinance to the Board, the
4 Department must first approve the policy, submit the policy to the City Attorney for review, and submit
5 the policy to the Mayor.

6
7 **SEC. 19B.4. STANDARD FOR APPROVAL.**

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

14
15 **SEC. 19B.5. COMPLIANCE FOR EXISTING SURVEILLANCE TECHNOLOGY.**

16 (a) Each Department possessing or using Surveillance Technology before the effective date of
17 this Chapter 19B shall submit a proposed Surveillance Technology Policy ordinance to the Board of
18 Supervisors for that particular Surveillance Technology no later than 120 days following the effective
19 date of this Chapter, for review and approval by the Board by ordinance.

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

1 (c) If the Board has not approved a Surveillance Technology Policy ordinance for Surveillance
2 Technology in use before the effective date of this Chapter 19B, within 180 days of its submission to the
3 Board, the Department shall cease its use of the Surveillance Technology and the sharing of data from
4 the Surveillance Technology until such time as the Board approves the Surveillance Technology Policy
5 ordinance in accordance with this Chapter.

6
7
8 **SEC. 19B.6. ANNUAL SURVEILLANCE REPORT.**

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

16 (b) By no later than January 15 of each fiscal year, each Department that has obtained
17 approval for the acquisition of Surveillance Technology under Section 19B.2 shall submit to the Board
18 of Supervisors a report regarding implementation of the policy and a resolution to accept the report.

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

23
24 **SEC. 19B.7. USE OF SURVEILLANCE TECHNOLOGY IN EXIGENT**
25 **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) for a**
2 **purpose or in a manner that is specifically prohibited in a Board-approved Surveillance Technology**
3 **Policy ordinance, or (2) without complying with the terms of this Chapter 19B. Unless otherwise**
4 **prohibited by law, the District Attorney may prosecute a violation of this Chapter.**

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

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

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

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

17
18 Section 3. The Administrative Code is hereby amended by revising Sections 2A.20 and
19 10.170-1, and adding Sections 3.27 and 21.07, to read as follows:

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

22 **(a)** The Controller shall audit the accounts of all boards, officers, and employees of the
23 City and County charged in any manner with the custody, collection, or disbursement of funds.
24 The Controller shall audit all accounts of money coming into the hands of the Treasurer, the
25 frequency of which shall be governed by State law.

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

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

8 **(d) Surveillance Technology Audit.**

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

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

22
23 **SEC. 10.170-1. GRANT FUNDS – ACCEPTANCE AND EXPENDITURE.**
24
25

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 I.

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
20 **SEC. 3.27. APPROPRIATIONS FOR SURVEILLANCE TECHNOLOGY.**

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

24 (b) To the extent that a Department seeks funding to acquire Surveillance Technology, the
25 Department shall transmit a Surveillance Technology Policy, approved by the Board of Supervisors in

1 accordance with Chapter 19B of the Administrative Code, with any budget estimate submitted to the
2 Controller in accordance with Section 3.3(a) or 3.15 of the Administrative Code. To the extent the
3 Mayor concurs in the funding request and the Surveillance Technology Policy, the Mayor shall include
4 the Surveillance Technology Policy with the proposed budget submitted to the Board of Supervisors in
5 accordance with Section 3.3(c) or (d) of the Administrative Code, or, in the case of a supplemental
6 appropriation, Section 3.15 of the Administrative Code.

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

19
20 ///

21 ///

22 ///

23 ///

24 ///

1 Section 4. Scope of Ordinance. In enacting this ordinance, the Board of Supervisors
2 intends to amend only those words, phrases, paragraphs, subsections, sections, articles,
3 numbers, punctuation marks, charts, diagrams, or any other constituent parts of the Municipal
4 Code that are explicitly shown in this ordinance as additions, deletions, Board amendment
5 additions, and Board amendment deletions in accordance with the "Note" that appears under
6 the official title of the ordinance.

7
8
9 APPROVED AS TO FORM:
10 DENNIS J. HERRERA, City Attorney

11 By:

12 
 JANA CLARK
 Deputy City Attorney

13 n:\legana\as2019\1900073\01334300.docx
14
15
16
17
18
19
20
21
22
23
24
25

LEGISLATIVE DIGEST

[Administrative Code - Acquisition of Surveillance Technology]

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.

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 to create and submit with any funding request a Surveillance Technology Policy ordinance, approved by the Board of Supervisors, setting forth a description of 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, who will be authorized

access, training, access controls, complaint procedures, and any safeguards to reduce the chilling effect of the technology and prevent its unauthorized use. This ordinance also would prohibit departments' use of surveillance technology services or equipment unless the Board of Supervisors had approved a Surveillance Technology Policy ordinance for the services or equipment. 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.

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.

n:\legana\as2019\1900073\01334009.docx



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 (authorizing 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.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB1186#.

¹⁴ A 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

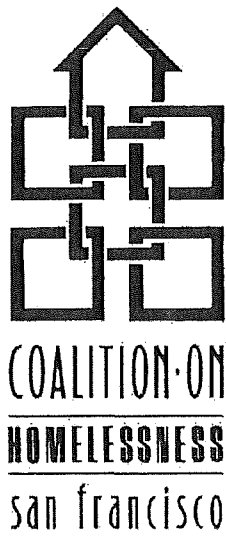
President Norman Yee
 Supervisor Sandra Lee Fewer
 Supervisor Catherine Stefani
 Supervisor Aaron Peskin
 Supervisor Gordon Mar
 Supervisor Vallie Brown
 Supervisor Matt Haney
 Supervisor Rafael Mandelman
 Supervisor Hillary Ronen
 Supervisor Shamann Walton
 Supervisor Ahsha Safai

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 b.



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.

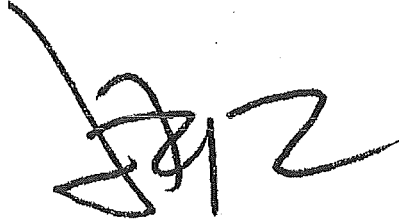
While arguments can, and have, been made about the benefits of surveillance technology to protect public safety, we strongly believe such technologies need to be regulated, and in the case of Facial Recognition technology, prohibited. There is no place in the City and County of San Francisco for the 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 be 'JF' followed by a stylized '12' or similar flourish.

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

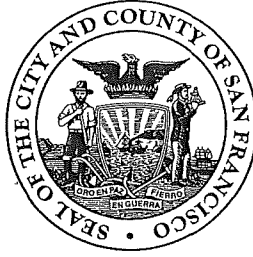
This ordinance is urgently needed given the onslaught of new surveillance technologies now available and the lack of regulation on the topic. By taking this important step, the City and County of San Francisco would be leading the nation as one of the first jurisdictions to ban facial-recognition technology 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, which appears to read "Cindy Myers", is positioned below the word "Sincerely,".

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 *[Signature]*
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):

- ☒ 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: []

