

**PROPOSED INITIATIVE ORDINANCE TO BE SUBMITTED BY FOUR OR MORE SUPERVISORS TO THE VOTERS AT THE JUNE 7, 2022 ELECTION.**

[Under Charter Section 2.113(b), this measure must be submitted to the Board of Supervisors and filed with the Department of Elections no less than *45 days prior* to deadline for submission of such initiatives to the Department of Elections set in Municipal Elections Code Section 300(b).]

[Initiative Ordinance – Administrative Code – Acquisition and Use of Surveillance Technology]

**Ordinance amending the Administrative Code to adopt, with minor changes, as a voter-approved measure, the ordinance which currently requires 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 or policies 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; requires 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 requires 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; and to**

permit amendment of the ordinance by the Board of Supervisors if consistent with the purposes of the ordinance.

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. This ordinance shall be known as the “Safe Communities and Transparent Government Act of 2022.”

Section 2. The voters hereby re-authorize and re-enact Chapter 19B of the Administrative Code, in the process adding Section 19B.11 and revising Sections 19B.1, 19B.2 and 19B.3, to read as follows:

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

**SEC. 19B.1. DEFINITIONS.**

“Annual Surveillance Report” means a written report that includes all of the following:

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

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

(3) A summary of complaints or concerns from the public about the Surveillance

Technology item;

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

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

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

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

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

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

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

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

An Annual Surveillance Report shall not contain the specific records that a Surveillance Technology item collects, stores, exchanges, or analyzes and/or information protected, restricted,

and/or sealed pursuant to State and/or federal laws, including information exempt from disclosure under the California Public Records Act.

“City” means the City and County of San Francisco.

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

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

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

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

“COIT” means the Committee on Information Technology.

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

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

“Surveillance Impact Report” means a written report that includes at a minimum the following:

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

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

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

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

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

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

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

“Personal communication device” means a cellular telephone that has not been modified beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.

“Protected Class” means a class of persons with shared characteristics based on sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, gender identity, gender expression, or sexual orientation, or any other class protected under the California Unruh Civil Rights Act.

“Surveillance Technology” means any software, electronic device, system utilizing an electronic device, or similar device used, designed, or primarily intended to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or similar information specifically associated with, or capable of being associated with, any individual or group. Surveillance Technology” includes but is not limited to the following: international mobile subscriber identity

(IMSI) catchers and other cell site simulators; automatic license plate readers; electric toll readers; closed-circuit television cameras; gunshot detection hardware and services; video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; mobile DNA capture technology; biometric software or technology, including facial, voice, iris, and gait recognition software and databases; software designed to monitor social media services; x-ray vans; software designed to forecast criminal activity or criminality; radio-frequency I.D. (RFID) scanners; and tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network. Surveillance Technology does not include the following devices, hardware, or software:

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

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

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

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

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

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

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

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

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

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

(11) Parking Ticket Devices;

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

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

(14) Police department early warning systems; and

(15) Computers, software, hardware, or devices intended to be used solely to monitor the safety and security of City facilities and City vehicles, not generally accessible to the public.

“Surveillance Technology Policy” means a written policy that includes:

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

~~(d) Notwithstanding the provisions of this Chapter 19B, it shall be unlawful for any Department to obtain, retain, access, or use: 1) any Face Recognition Technology on a City-issued product or device; or 2) any information obtained from Face Recognition Technology on City-issued software or a City-issued product or device. This subsection (d) is subject to the exceptions in subsections (e)-(g) and the qualifications in subsections (h)-(l).~~

~~(e) A Department's inadvertent or unintentional receipt, retention, access to, or use of any information obtained from Face Recognition Technology shall not be a violation of this subsection (d), provided that:~~

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

~~\_\_\_\_\_ (2) The Department logs such receipt, access to, or use in its Annual Surveillance Report.~~

~~\_\_\_\_\_ (f) It shall not be a violation of subsection (d) for a City Department to possess Face Recognition Technology on City issued software or a City issued product or device, provided that:~~

~~\_\_\_\_\_ (1) The Face Recognition Technology is a stock, manufacturer installed capability, bundled with software or stored on a product or device, and that the functions unrelated to Face Recognition Technology are necessary to perform essential City functions;~~

~~\_\_\_\_\_ (2) The software, product, or device was not acquired for the purpose of performing the Face Recognition Technology function;~~

~~\_\_\_\_\_ (3) The Face Recognition Technology cannot be deleted from the software, product, or device; and~~

~~\_\_\_\_\_ (4) The Department does not use the Face Recognition Technology.~~

~~\_\_\_\_\_ (g) It shall not be a violation of subsection (d) to acquire or obtain a software, product, or device that includes Face Recognition Technology provided that:~~

~~\_\_\_\_\_ (1) In advance of obtaining the software, product, or device, the Department makes a written finding that the software, product, or device is not being acquired or obtained for the purpose of performing the Face Recognition Technology Function;~~

~~\_\_\_\_\_ (2) In advance of obtaining the software, product, or device, the Purchaser or the Purchaser's designee makes a written finding that the Face Recognition Technology is a stock, manufacturer installed capability bundled with software, or stored on a product or device; that the functions unrelated to Face Recognition Technology are necessary to perform essential City functions; and that the software, product, or device is unavailable without the stock, manufacturer installed Face Recognition Technology; and~~

~~\_\_\_\_\_ (3) The City Department obtains approval of a Surveillance Technology Ordinance under this Chapter 19B where the software, product, or device constitutes Surveillance Technology.~~

~~\_\_\_\_\_ (h) A City Department that possesses Face Recognition Technology shall certify compliance with subsections (e) - (l) and post that certification and the written findings required by subsection (g) on the Department website.~~

~~\_\_\_\_\_ (i) If either the District Attorney or Sheriff certifies in writing to the Controller that acquisition of Surveillance Technology is necessary to perform an investigative or prosecutorial function and provides in writing to the Controller either an explanation of how compliance with this Chapter 19B will obstruct their investigative or prosecutorial function or a declaration that the explanation itself will obstruct either function, the District Attorney or Sheriff shall simultaneously submit a copy of the document to the Clerk of the Board of Supervisors so that the Board in its discretion may hold a hearing and request that the District Attorney or Sheriff appear to respond to the Board's questions regarding such certification, explanation, and/or declaration. The written certification shall specify the Surveillance Technology acquired, or to be acquired.~~

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

~~(k) Except as restricted by subsection 19B.2(d) or expressly restricted in a Surveillance Technology Policy developed pursuant to subsection 19B.2(a)(5), nothing in this Chapter 19B shall be construed to prohibit, restrict, or interfere with the receipt, access to, or use by a City department of information gathered by a non-City entity or individual from Surveillance Technology.~~

~~(l) Nothing in this Chapter 19B shall prohibit, restrict, or interfere with a Department's use of Surveillance Technology to conduct internal investigations involving City employees, contractors, and volunteers, or the City Attorney's ability to receive or use, in preparation for or in civil or administrative proceedings, information from Surveillance Technology (excluding Face Recognition~~

Technology to the extent prohibited under section 19B.2.d) that any City agency, department or official gathers or that any other non-City entity or person gathers.

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

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

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

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

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

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

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

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

(b) Each Department possessing or using Surveillance Technology before the effective date of this Chapter 19B shall submit a proposed Surveillance Technology Policy ordinance to the Board of Supervisors, in accordance with the procedures set forth in subsection 19B.2(b), for each particular Surveillance Technology no later than 180 days following the effective date of this Chapter, for review and approval by the Board by ordinance. A Department may submit a Surveillance Technology Policy ordinance that includes multiple, separate policies for each particular Surveillance Technology possessed or used before the effective date of this Chapter 19B.

(c) If a Department is unable to meet this 180-day timeline, the Department may notify the COIT in writing of the Department's request to extend this period and the reasons for that request. COIT may for good cause grant a Department extensions of up to 90 days per extension, beyond the 180-day timeline to submit a proposed Surveillance Technology Policy.

(d) Each Department possessing or using Surveillance Technology before the effective date of this Chapter 19B may continue its use of the Surveillance Technology and the sharing of data from the Surveillance Technology until such time as the Board enacts an ordinance regarding the Department's Surveillance Technology Policy and such ordinance becomes effective under Charter Section 2.105.

#### **SEC. 19B.6. ANNUAL SURVEILLANCE REPORT.**

(a) A Department that obtains approval for the acquisition of Surveillance Technology under Section 19B.2 must submit to the Board of Supervisors and COIT, and make available on its website, an Annual Surveillance Report for each Surveillance Technology used by the City Department within 12 months of Board approval of the applicable Surveillance Technology Policy, and annually thereafter on or before November 1. If the Department is unable to meet the deadline, the Department

~~may submit a request to COIT for an extension of the deadline. COIT may extend the deadline for good cause.~~

~~(b) By no later than February 15 of each year, each Department that has obtained approval for the acquisition of Surveillance Technology under Section 19B.2 shall submit to the Board of Supervisors the Department's Annual Surveillance Report and a resolution to accept the report.~~

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

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

#### **SEC. 19B.7. USE OF SURVEILLANCE TECHNOLOGY IN EXIGENT**

##### **CIRCUMSTANCES.**

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

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

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

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

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

(5) Submit a written report summarizing that acquisition and/or use of Surveillance Technology under this Section 19B.7 to the Board of Supervisors within 60 days following the inception of the exigent circumstances.

(b) Any Surveillance Technology temporarily acquired in exigent circumstances shall be returned within 7 days following the conclusion of the exigent circumstances, unless the Department acquires the Surveillance Technology in accordance with the requirements of this Chapter 19B.

#### **SEC. 19B.8. ENFORCEMENT.**

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

(b) Any alleged violation of this Chapter 19B for which the City received notice under subsection (c) and that is not corrected by the Department within 30 days of receipt of the notice, constitutes a legally cognizable basis for relief, and any person affected thereby may institute proceedings for injunctive relief, declaratory relief, or writ of mandate to remedy the violation, in any court of competent jurisdiction to enforce this Chapter 19B. An action instituted under this subsection (b) shall be brought against the City.

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



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

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

**SEC. 19B.9. IMPLEMENTING STANDARDS.**

After notice and a public hearing, the City Administrator or the City Administrator's designee is authorized to adopt or amend rules, regulations, operational standards and interpretative guidelines ("Implementing Standards") that are not inconsistent with this Chapter 19B or its purposes and that will assist and guide departments in implementing this Chapter. An Implementing Standard adopted under this Section 19B.9 shall not become operative until 10 days after the notice of the adoption is posted on the City Administrator's website. The Implementing Standard shall cease to be operative if an ordinance referring to the specific Implementing Standard and proposing to address the same subject matter as that Implementing Standard is introduced at the Board of Supervisors.

**SEC. 19B.10. POSTING OF BOARD-APPROVED SURVEILLANCE TECHNOLOGY POLICIES; APPENDIX.**

(a) Each Department shall post each Surveillance Technology Policy for that Department that has been approved by the Board of Supervisors in accordance with this Chapter 19B, on the Department's website within 10 days of the Board's approval of the policy.

(b) There shall be an Appendix to this Chapter 19B, which shall contain a record of all Surveillance Technology Policies approved by the Board of Supervisors in accordance with this Chapter 19B. Upon approval by ordinance of a Surveillance Technology Policy, the City Attorney shall cause said policy to be identified in said Appendix.

## **CHAPTER 19B: ACQUISITION OF SURVEILLANCE TECHNOLOGY**

### **SEC. 19B.1. DEFINITIONS.**

“Annual Surveillance Report” means a written report that includes all of the following:

- (1) A general description of how the Surveillance Technology was used;
- (2) A general description of whether and how often data acquired through the use of the Surveillance Technology item was shared with outside entities, the name of any recipient outside entity, the type(s) of data disclosed, under what legal standard(s) the data was disclosed, and the justification for the disclosure(s);
- (3) A summary of complaints or concerns from the public about the Surveillance Technology item;
- (4) The aggregate results of any internal audits required by the Surveillance Technology Policy, any general, aggregate information about violations of the Surveillance Technology Policy, and a general description of any actions taken in response;
- (5) Information, including crime statistics, which help the Board of Supervisors assess whether the Surveillance Technology has been effective at achieving its identified purposes;
- (6) Aggregate statistics and information about any Surveillance Technology related to Public Records Act requests;
- (7) Total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source of funding will fund the Surveillance Technology in the coming year;
- (8) Any requested modifications to the Surveillance Technology Policy and a detailed basis for the request;

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

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

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

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

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

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

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

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

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

“COIT” means the Committee on Information Technology.

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

“Face recognition technology” means an automated or semi-automated process that assists in identifying or verifying an individual, or captures information about them, based on an individual's face.

“Surveillance Impact Report” means a written report that includes at a minimum the following:

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

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

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

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

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

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

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

“Personal communication device” means a cellular telephone that has not been modified beyond stock manufacturer capabilities, a personal digital assistant, a wireless capable tablet or similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.

“Protected Class” means a class of persons with shared characteristics based on sex, race, color, religion, ancestry, national origin, disability, medical condition, genetic information, marital status, gender identity, gender expression, or sexual orientation, or any other class protected under the California Unruh Civil Rights Act.

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

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

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

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

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

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

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

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

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

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

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

(11) Parking Ticket Devices;

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

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

(14) Police department early warning systems; and

(15) Computers, software, hardware, or devices intended to be used solely to monitor the safety and security of City facilities and City vehicles, not generally accessible to the public.

“Surveillance Technology Policy” means a written policy that includes:

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

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

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

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

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

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

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

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

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

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

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

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



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

**TECHNOLOGY POLICY.**

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

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

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

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

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

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

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

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

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

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

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

(d) Notwithstanding the provisions of this Chapter 19B, it shall be unlawful for any Department to obtain, retain, access, or use: 1) any Face Recognition Technology; or 2) any information obtained from Face Recognition Technology. This subsection (d) is subject to the exceptions in subsections (e)-(g) and the qualifications in subsections (h)-(l).

(e) A Department's inadvertent or unintentional receipt, retention, access to, or use of any information obtained from Face Recognition Technology shall not be a violation of this subsection (d), provided that:

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

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

(f) It shall not be a violation of subsection (d) for a City Department to possess Face Recognition Technology on City-issued software or a City-issued product or device, provided that:

(1) The Face Recognition Technology is a stock, manufacturer-installed capability, bundled with software or stored on a product or device, and that the functions unrelated to Face Recognition Technology are necessary to perform essential City functions;

(2) The software, product, or device was not acquired for the purpose of performing the Face Recognition Technology function;

(3) The Face Recognition Technology cannot be deleted from the software, product, or device; and

(4) The Department does not use the Face Recognition Technology.

(g) It shall not be a violation of subsection (d) to acquire or obtain a software, product, or device that includes Face Recognition Technology provided that:

(1) In advance of obtaining the software, product, or device, the Department makes a written finding that the software, product, or device is not being acquired or obtained for the purpose of performing the Face Recognition Technology Function;

(2) In advance of obtaining the software, product, or device, the Purchaser or the Purchaser's designee makes a written finding that the Face Recognition Technology is a stock, manufacturer-installed capability bundled with software, or stored on a product or device; that the functions unrelated to Face Recognition Technology are necessary to perform essential City functions; and that the software, product, or device is unavailable without the stock, manufacturer-installed Face Recognition Technology; and

(3) The City Department obtains approval of a Surveillance Technology Ordinance under this Chapter 19B where the software, product, or device constitutes Surveillance Technology.

(h) A City Department that possesses Face Recognition Technology shall certify compliance with subsections (e)-(l) and post that certification and the written findings required by subsection (g) on the Department website.

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

hearing and request that the District Attorney or Sheriff appear to respond to the Board's questions regarding such certification, explanation, and/or declaration. The written certification shall specify the Surveillance Technology acquired, or to be acquired.

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

(k) Except as restricted by subsection 19B.2(d) or expressly restricted in a Surveillance Technology Policy developed pursuant to subsection 19B.2(a)(5), nothing in this Chapter 19B shall be construed to prohibit, restrict, or interfere with the receipt, access to, or use by a City department of information gathered by a non-City entity or individual from Surveillance Technology.

(l) Nothing in this Chapter 19B shall prohibit, restrict, or interfere with a Department's use of Surveillance Technology to conduct internal investigations involving City employees, contractors, and volunteers, or the City Attorney's ability to receive or use, in preparation for or in civil or administrative proceedings, information from Surveillance Technology (excluding Face Recognition Technology to the extent prohibited under section 19B.2.d) that any City agency, department or official gathers or that any other non-City entity or person gathers.

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

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

(b) The Department seeking approval under Section 19B.2 shall submit to the Board of Supervisors a Surveillance Impact Report and a proposed Surveillance Technology Policy ordinance at

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

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

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

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

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

(b) Each Department possessing or using Surveillance Technology before the effective date of this Chapter 19B shall submit a proposed Surveillance Technology Policy ordinance to the Board of Supervisors, in accordance with the procedures set forth in subsection 19B.2(b), for each particular Surveillance Technology no later than 180 days following the effective date of this Chapter, for review and approval by the Board by ordinance. A Department may submit a Surveillance Technology Policy ordinance that includes multiple, separate policies for each particular Surveillance Technology possessed or used before the effective date of this Chapter 19B.

(c) If a Department is unable to meet this 180-day timeline, the Department may notify the COIT in writing of the Department's request to extend this period and the reasons for that request.

COIT may for good cause grant a Department extensions of up to 90 days per extension, beyond the 180-day timeline to submit a proposed Surveillance Technology Policy.

(d) Each Department possessing or using Surveillance Technology before the effective date of this Chapter 19B may continue its use of the Surveillance Technology and the sharing of data from the Surveillance Technology until such time as the Board enacts an ordinance regarding the Department's Surveillance Technology Policy and such ordinance becomes effective under Charter Section 2.105.

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

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

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

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

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

**SEC. 19B.7. USE OF SURVEILLANCE TECHNOLOGY IN EXIGENT**

**CIRCUMSTANCES.**

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

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

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

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

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

*(5) Submit a written report summarizing that acquisition and/or use of Surveillance Technology under this Section 19B.7 to the Board of Supervisors within 60 days following the inception of the exigent circumstances.*

*(b) Any Surveillance Technology temporarily acquired in exigent circumstances shall be returned within 7 days following the conclusion of the exigent circumstances, unless the Department acquires the Surveillance Technology in accordance with the requirements of this Chapter 19B.*

**SEC. 19B.8. ENFORCEMENT.**

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

(b) Any alleged violation of this Chapter 19B for which the City received notice under subsection (c) and that is not corrected by the Department within 30 days of receipt of the notice, constitutes a legally cognizable basis for relief, and any person affected thereby may institute proceedings for injunctive relief, declaratory relief, or writ of mandate to remedy the violation, in any court of competent jurisdiction to enforce this Chapter 19B. An action instituted under this subsection (b) shall be brought against the City.

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

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

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

#### **SEC. 19B.9. IMPLEMENTING STANDARDS.**

After notice and a public hearing, the City Administrator or the City Administrator's designee is authorized to adopt or amend rules, regulations, operational standards and interpretative guidelines ("Implementing Standards") that are not inconsistent with this Chapter 19B or its purposes and that will assist and guide departments in implementing this Chapter. An Implementing Standard adopted under this Section 19B.9 shall not become operative until 10 days after the notice of the adoption is posted on the City Administrator's website. The Implementing Standard shall cease to be operative if



an ordinance referring to the specific Implementing Standard and proposing to address the same subject matter as that Implementing Standard is introduced at the Board of Supervisors.

**SEC. 19B.10. POSTING OF BOARD-APPROVED SURVEILLANCE TECHNOLOGY POLICIES; APPENDIX.**

(a) Each Department shall post each Surveillance Technology Policy for that Department that has been approved by the Board of Supervisors in accordance with this Chapter 19B, on the Department's website within 10 days of the Board's approval of the policy.

(b) There shall be an Appendix to this Chapter 19B, which shall contain a record of all Surveillance Technology Policies approved by the Board of Supervisors in accordance with this Chapter 19B. Upon approval by ordinance of a Surveillance Technology Policy, the City Attorney shall cause said policy to be identified in said Appendix.

**SEC. 19B.11. AMENDMENT OF ORDINANCE.**

The voters may amend or repeal this Chapter 19B. The Board of Supervisors may only amend this Chapter 19B if the amendment furthers the purposes of this Chapter, which are to protect the public from surveillance and safeguard civil rights and civil liberties.

Section 3. Conflicting Ballot Measures. In the event that this measure and another measure relating to the use of surveillance technology shall appear on the same municipal election ballot, the provisions of such other measure shall be deemed in conflict with this measure. In the event that this measure shall receive a greater number of affirmative votes, the provisions of this measure shall prevail in their entirety and each and every provision of

the other measure that conflicts, in whole or in part, with this measure shall be null and void in their entirety.

Section 4. Severability. If any section, subsection, sentence, clause, phrase, or word of this ordinance, or any application thereof to any person or circumstance, is held to be invalid or unconstitutional by a decision of a court of competent jurisdiction, such decision shall not affect the validity of the remaining portions or applications of this ordinance.

Section 5. Effective Date. The effective date of this ordinance shall be ten days after the date the official vote count is declared by the Board of Supervisors.

\* \* \*

SUBMITTED.

Caron Pashin Date: \_\_\_\_\_  
Member, Board of Supervisors

\_\_\_\_\_ Date: \_\_\_\_\_  
Member, Board of Supervisors

\_\_\_\_\_ Date: \_\_\_\_\_  
Member, Board of Supervisors

\_\_\_\_\_ Date: \_\_\_\_\_  
Member, Board of Supervisors