Privacy & Surveillance Advisory Board

Regular Meeting

November 22, 2019

1 Dr. Carlton B. Goodlett Place, City Hall, Room 400
San Francisco, CA 94102

Agenda

- Call to Order by Chair
- Roll Call
- Welcome by PSAB Chair
- Review of Section 19B & Surveillance Inventory
- Discussion: Exempt Surveillance Technologies
- Implementing Standards for Impact Report and Surveillance Technology Policy (Action Item)
- Public Comment
- Adjournment

3. Welcome by PSAB Chair

Mission

- Review Ordinance Requirements
- Make Recommendations to the City Administrator
- Support a Public Dialogue on Privacy

Types of Action Items

1. Ordinance Requirements
   - Impact Report
   - Surveillance Technology Policy
2. Implementing Standards
3. Ordinance Amendments

Logistics

Meeting Frequency

- 2nd and 4th Friday of each month
- Meetings will only occur as needed (currently 186 surveillance technologies must be processed)

4. Review of Section 19B & Surveillance Inventory

Ordinance Overview

- Purpose of Ordinance
- Legislative History
- Surveillance Technology Defined
- Ordinance Requirements
- Inventory Overview

Purpose of Ordinance

- Promote Transparency
- Protect privacy rights of residents and business
- Initiate a public discussion on government surveillance

Legislative History

Legislative History

May 31, 2019 – Version 1 enacted	*COIT to draft Surveillance Technology Policies on departments' behalf*
June 14, 2019 – Version 2 enacted	*COIT authorized to grant Surveillance Technology Policy extensions*
September 10, 2019 – Version 3 introduced	*Facial Recognition Technology Amendment & City Administrator authorized to adopt and amend the Ordinance's Implementing Standards**

**Implementing Standards = rules, operational standards and interpretive guidelines that assist and guide departments through Ordinance implementation*

Surveillance Technology Defined

“Surveillance Technology” is

a) Any software, electronic device, system utilizing an electronic device, or similar device used, designed, or primarily intended to
b) Collect, retain, process, or share
c) Audio, electronic, visual, location, thermal, biometric, olfactory or similar information
d) Associated with, or capable of being associated with, any individual or group

...with 15 exemptions

Otherwise stated:

- ✓ A “Surveillance Technology” is any technology used to collect information on any individual or group.

Ordinance Requirements

Ordinance Requirements

For current or proposed surveillance technologies, departments must complete:

1. **Surveillance Technology Inventory –** due to COIT August 29, 2019
2. **Reporting Requirements:**
    a) **Surveillance Impact Report** – submitted to COIT
    b) **Surveillance Technology Policy** - approved by COIT and Dept leadership, reviewed by City Attorney, and submitted to the Board of Supervisors by December 27, 2019
    c) **Annual Surveillance Report** – due starting May 31, 2020

Ordinance Requirements

Requirement	Description	Items
Surveillance Impact Report	An assessment of the benefits, costs, privacy, and civil rights impacts.	7
Surveillance Technology Policy	Establishes rules of operations to safeguard privacy and civil rights.	12
Annual Surveillance Report	Continued analysis of impacts and public response to ongoing use	11

Surveillance Impact Report	Surveillance Technology Policy	Annual Surveillance Report
At a minimum, must include 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 anticipated costs, failures, or civil rights and civil liberties abuses.	Must include the below: (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.	Must include 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; (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, exchanged, or analyzes and/or information protected, restricted, and/or sealed pursuant to the State and/or federal laws, including information exempt from disclosure under the California Public Records Act.

Inventory Overview

Inventory Overview

A total of **186** technologies identified thus far:

- 74 technologies (40%) possibly exempt
- The remaining 112 (60%) should proceed to complete Impact Reports and Surveillance Policies

5. Discussion: Exempt Surveillance Technologies

Inventory Overview

A total of **186** technologies identified thus far:

- 74 technologies (40%) possibly exempt
- The remaining 112 (60%) should proceed to complete Impact Reports and Surveillance Policies

Inventory Exemptions

- **Exemption 1** - Office hardware in common use by City Departments and used for routine City business & transactions (i.e. TVs, computers, credit card machines, copy machines, telephones, printers, etc.)
- **Exemption 2** - City databases and enterprise systems that contain information kept in the ordinary course of City business (i.e. human resources, permit, license, and business records)
- **Exemption 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 (i.e. payroll, accounting, or other fiscal databases)
- **Exemption 4** - Information technology security systems, including firewalls and other cybersecurity systems intended to secure City data
- **Exemption 5** - Physical access control systems, employee identification management systems, and other physical control systems
- **Exemption 6** - Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, electrical, natural gas, or water or sewer functions
- **Exemption 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
- **Exemption 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

Inventory Exemptions continued…

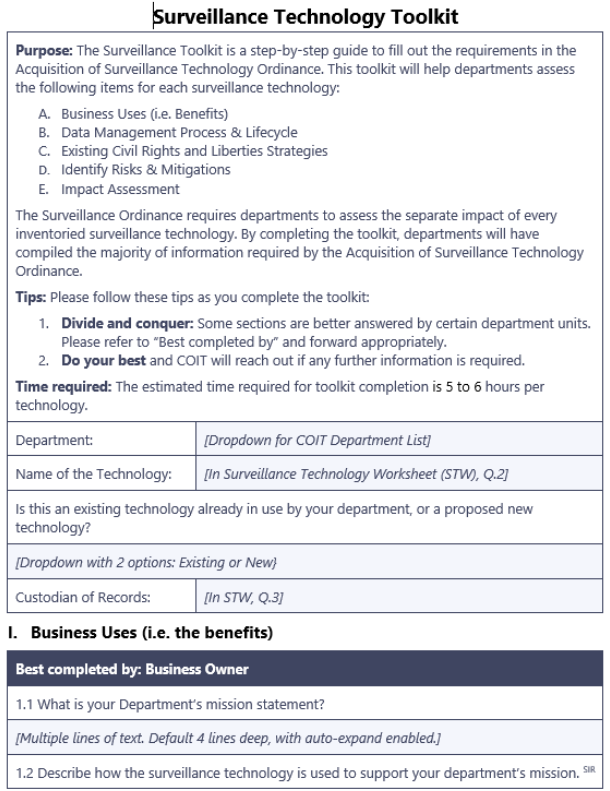
- **Exemption 9** - Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision equipment
- **Exemption 10** - Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury, and used and/or kept in the ordinary course of providing City services
- **Exemption 11** - Parking Ticket Devices
- **Exemption 12** - Police Department interview rooms, holding cells, and internal security audio/video recording systems
- **Exemption 13** - Police department computer aided dispatch (CAD), records/case management, Live Scan, booking, DMV, California Law Enforcement Telecommunications Systems (CLETS), 9-1-1 and related dispatch and operation or emergency services systems
- **Exemption 14** - Police department early warning systems
- **Exemption 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.

6. Implementing Standards for Impact Report and Surveillance Technology Policy (Action Item)

Surveillance Technology Toolkit

COIT's Toolkit aims to achieve:

- A robust impact assessment
- A standard structure to streamline department completion of all Ordinance requirements
- Minimize departments' implementation burden
- Inform the Board of Supervisors' decision assessing whether the benefits of each surveillance technology outweigh the costs.



Surveillance Technology Toolkit

Purpose: The Surveillance Toolkit is a step-by-step guide to fill out the requirements in the Acquisition of Surveillance Technology Ordinance. This toolkit will help departments assess the following items for each surveillance technology:

A. Business Uses (i.e. Benefits)
B. Data Management Process & Lifecycle
C. Existing Civil Rights and Liberties Strategies
D. Identify Risks & Mitigations
E. Impact Assessment

The Surveillance Ordinance requires departments to assess the separate impact of every inventoried surveillance technology. By completing the toolkit, departments will have compiled the majority of information required by the Acquisition of Surveillance Technology Ordinance.

Tips: Please follow these tips as you complete the toolkit:

1. **Divide and conquer:** Some sections are better answered by certain department units. Please refer to "Best completed by" and forward appropriately.
2. **Do your best** and COIT will reach out if any further information is required.

Time required: The estimated time required for toolkit completion is 5 to 6 hours per technology.

Department:	*[Dropdown for COIT Department List]*
Name of the Technology:	*[In Surveillance Technology Worksheet (STW), Q.2]*
Is this an existing technology already in use by your department, or a proposed new technology?	
[Dropdown with 2 options: Existing or New]	
Custodian of Records:	*[In STW, Q.3]*

I. Business Uses (i.e. the benefits)

Best completed by: Business Owner
1.1 What is your Department's mission statement?
[Multiple lines of text. Default 4 lines deep, with auto-expand enabled.]
1.2 Describe how the surveillance technology is used to support your department's mission. SIR

Surveillance Technology Toolkit

Primary Features:

- Definition of Authorized Use Case
- Match financial information to COIT budget process
- Interpretation on how to assess civil liberties and civil rights impacts
- Data Management Lifecycle – incorporated definitions and guidance from General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) among others.
- Use of COIT Data Classification Standard
- Identifies who is best positioned to answer questions

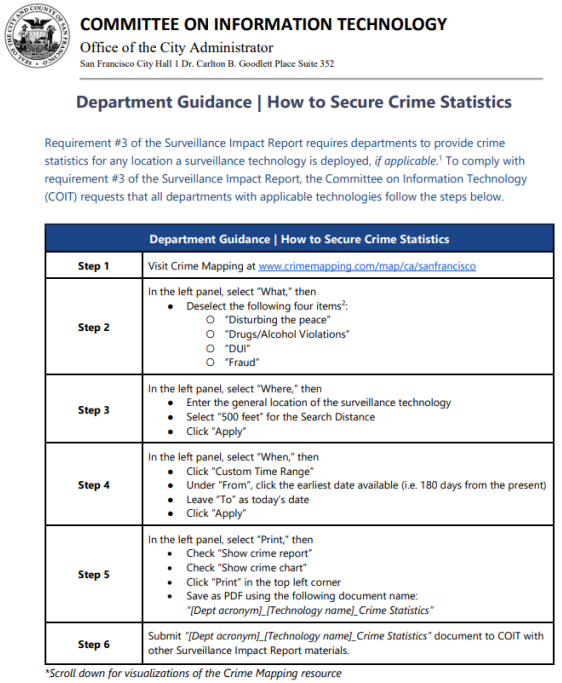
Crime Statistics Guidance

Surveillance Impact Requirement:

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

Staff recommendation:

- Guidance needed to ensure standard response.
- Data from crimemapping.com provided by San Francisco Police Department.



COMMITTEE ON INFORMATION TECHNOLOGY
Office of the City Administrator
San Francisco City Hall 1 Dr. Carlton B. Goodlett Place Suite 352

Department Guidance | How to Secure Crime Statistics

Requirement #3 of the Surveillance Impact Report requires departments to provide crime statistics for any location a surveillance technology is deployed, *if applicable*.[1] To comply with requirement #3 of the Surveillance Impact Report, the Committee on Information Technology (COIT) requests that all departments with applicable technologies follow the steps below.

Department Guidance | How to Secure Crime Statistics	
Step 1	Visit Crime Mapping at www.crimemapping.com/map/ca/sanfrancisco
Step 2	In the left panel, select "What," then • Deselect the following four items[2]: ○ "Disturbing the peace" ○ "Drugs/Alcohol Violations" ○ "DUI" ○ "Fraud"
Step 3	In the left panel, select "Where," then • Enter the general location of the surveillance technology • Select "500 feet" for the Search Distance • Click "Apply"
Step 4	In the left panel, select "When," then • Click "Custom Time Range" • Under "From", click the earliest date available (i.e. 180 days from the present) • Leave "To" as today's date • Click "Apply"
Step 5	In the left panel, select "Print," then • Check "Show crime report" • Check "Show crime chart" • Click "Print" in the top left corner • Save as PDF using the following document name: *"[Dept acronym]_[Technology name]_Crime Statistics"*
Step 6	Submit *"[Dept acronym]_[Technology name]_Crime Statistics"* document to COIT with other Surveillance Impact Report materials.

**Scroll down for visualizations of the Crime Mapping resource*

7. Public Comment