# FACT SHEET
# "Stop Secret Surveillance Ordinance"
# & Facial Recognition Ban
# (Sup. Peskin)

**DESCRIPTION OF THE ORDINANCE:**

The "**Stop Secret Surveillance Ordinance"** requires public transparency and oversight of all decisions to seek, obtain. or use surveillance technologies by San Francisco City Departments. The bill applies to existing and new technologies and to all City Departments, including the police department, sheriff's department, and the district attorney.

The Ordinance would also ban any Department from obtaining, accessing or using any Facial Recognition Technology.

The bill also requires strict surveillance use policies for any technology acquired or used, as well as auditing and reporting to ensure compliance with those policies and the Ordinance.

**BACKGROUND**

The Ordinance would require a Department to seek Board of Supervisors' approval, by ordinance, of a **Surveillance Use Policy** prior to:

- Seeking funds for Surveillance Technology**;**
- Acquiring or borrowing new Surveillance Technology;
- Using new or existing Surveillance Technology for a purpose, in a manner, or in a location not already set forth in a Surveillance Use Policy; or
- Entering into an agreement with a non-City entity to acquire, share or otherwise use Surveillance Technology.

**The Ordinance** is an implementation vehicle of Supervisor Peskin's "Privacy First Policy" (Proposition B) which was overwhelmingly approved by voters in November 2018.

**The Ordinance would also ban the government use or acquisition of facial recognition technology.** The proposed ban comes on the heels of mounting concerns about the surveillance and public safety risks of the technology expressed by civil rights groups, members of U.S. Congress, shareholders, tech workers, and the industry itself. Numerous research studies have also demonstrated this technology is prone to misidentification and inaccuracy for women and people of color, amplifying the public safety risk posed by its deployment for already-vulnerable and frequently-profiled communities.

**Standard for Board of Supervisors Approval (Cost-Benefit Analysis):** The Board of Supervisors may only approve a Surveillance Technology if it determines that:

- the benefits of the Surveillance Technology outweigh the costs;
- that civil liberties and civil rights will be safeguarded;
- and that use of the Surveillance Technology will *not* have a disparate impact on any community or group.

**Annual Audit by the Controller's Office:** The Ordinance would also require an annual audit of the Surveillance Technology, including review of:
(1) whether the subject Department has been operating in compliance with an approved Surveillance Technology Policy;
(2) whether the subject Department has completed an Annual Surveillance Report; and
(3) the total cost of the Surveillance Technology to the Department.

The Ordinance applies to existing surveillance technology and requires City Departments in possession of such technologies to create surveillance use policies for those technologies and submit those policies to the Board. The bill includes a **120-day Compliance Window for existing Surveillance Technology**, which may be extended by up to 90 days. If the Board does not approve a submitted policy for an existing technology, a City Department must cease use of it until it is approved.

**DEFINITIONS:**

**"Surveillance Technology"** is broadly defined to includes "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."

An "**Annual Surveillance Report"** must include:

- A description of how the Surveillance Technology was ***used***;
- Whether and how often data was ***shared with outside entities***, including the name of any recipient entities, the type(s) of data disclosed, under what legal standard(s) the data was disclosed, and any other justification for the disclosure(s);
- A summary of **community complaints** about the Surveillance Technology;
- Aggregate information about any *violations* of the Surveillance Technology Policy and steps taken in response;
- Information, including crime statistics, which may help the Board assess ***whether the Surveillance Technology was effective*** at achieving its identified purpose;
- Any ***Public Records Act requests*** related to the Surveillance Technology;
- Total ***annual cost*** of the Surveillance Technology;
- Any ***requested modifications to the Surveillance Technology Policy*** and

the basis for any requested modification; and
- A general breakdown of any physical objects (i.e., hardware) that the Surveillance Technology was applied to, or, in the case of Surveillance Technology software, any data sets to which the software was applied.

A "**Surveillance Impact Report"** must include:
- Information describing how the Surveillance Technology works;
- The proposed purpose of the Surveillance Technology;
- Any locations where the Surveillance Technology is proposed to be deployed, and any crime statistics for those locations;
- An assessment of the potential impact on civil liberties and civil rights, and any plans to safeguard the rights of the public;
- The fiscal cost of the Surveillance Technology, including the initial purchase costs, personnel and other ongoing costs, and any current or potential sources of funding;
- Whether use or maintenance of the Surveillance Technology will require data to be handled or used by any third-party vendor; and
- A summary of any experience the Department has with the subject Surveillance Technology, including unanticipated costs, or civil rights or civil liberties abuses.

A "**Surveillance Technology Policy"** shall include:
- A description of the Surveillance Technology, including the data that might be collected by the Surveillance Technology;
- The purpose of the Surveillance Technology, including authorized uses and uses that are expressly prohibited;
- A description of the data formats;
- Specific categories of individuals authorized to access information collected by the Surveillance Technology, including circumstances in which access or use is allowed;
- Safeguards to prevent unauthorized access;
- Retention schedule for information collected by the Surveillance Technology;
- How information may be accessed by members of the public, including by criminal defendants;
- The training required for any individual authorized to access information;
- Steps that will be taken to ensure compliance with the Surveillance Technology Policy;
- What procedures will be put in place for members of the public to register complaints or concerns.