City of St. Louis Surveillance Systems and the Protection of Citizen Privacy Executive Order

Table of Contents

For the purposes of this policy the following Terms and Definitions apply

Authorized Access – Access approved by an authority allowed to grant access under this policy.

Back-End – Equipment and software that is used as part of a surveillance system that is not an edge device including things like servers, network equipment, and management software.

Biometrics – Technologies used to identify a specific individual based on the individual's physical characteristics such as facial recognition.

Biometric Data – All data including biometric profiles used during the application of biometrics to identify and individual. This also includes data derived from the use of biometrics such as the number of times and locations in which and individual was identified. Note: While surveillance data may be used for biometric identification the surveillance data is not considered biometric data.

Biometric Profile – The physical characteristic data used identify a specific individual based on the individual's physical characteristics.

Condition – Specific terms under which something can or cannot be done.

Surveillance Data – Information such as audio, video, and still images captured by a surveillance system and/or information captured regarding the use and status of a surveillance system.

Edge Device – The specific equipment or software used to capture surveillance data such as cameras and microphones.

End User / Internal User / User – A City employee that accesses a surveillance system and the data generated by the surveillance system.

Federation – The addition or inclusion of third-party back-end or edge devices owned, operated, managed, and maintained by a third party to City surveillance systems

Intended Use – The reasons for the use of surveillance technologies expressed as outcomes.

Key Performance Indicator (KPI) – A specific quantifiable indicator/measures used to determine the effectiveness of the use of surveillance systems to achieve desired outcomes.

Metrics – The measurement of the use of surveillance systems to achieve desired outcomes that may also be used to make data driven decisions regarding the continued use of a surveillance system or no longer using a surveillance system.

Outcome – A desired benefit or desired impact that is the reason for using a surveillance system.

Permissible Use – The ways a surveillance system can or cannot be used based on the intended use.

Personally Identifiable Information (PII) – Any information that could reasonably be used to identify a specific individual as also defined in OMB Memorandum M-07-1616 as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Public Employee – Any individual that is employed by the City of St. Louis including contractors and consultants.

Public Facilities – Any building owned, leased, or operated by the City (for example, City Hall and recreation centers).

Public Land – Any land or area owned or maintained by the City that is accessible to the general public (for example, parks).

Real-Time Video Stream – Video and/or audio data that is viewed or monitored as it is captured by an edge device (for example, live video)

Right-Of-Way – Areas available for use by the general public including, public streets, sidewalks, alleys, and land.

Substantive Revision – Any revision to this policy that adds a new, alters an existing, or eliminates an intended use, permissible use, and/or condition.

Surveillance System – Any system that is used to monitor behavior, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people and assets. This includes observation by means of electronic equipment.

Targeting – The use of a surveillance system to identify or track a specific individual or group of individuals.

Temporary – Less than thirty (30) days.

Third Party – Any entity that is not a City agency, board, or department covered by this policy.

Third Party End User / External User – Any entity that is not a city employee.

Unauthorized Access – Access not approved by an authority allowed to grant access under this policy.

Vacant and Problem Properties – Any property that meets the City's established definition of vacant or problem properties regardless of who owns the property.

Video Management System (VMS) – A system that serves any or all of the following functions:

- collects video from cameras and other sources,
- is used to configure, control, and monitor video devices,
- records / stores video or audio to a storage device, and/or
- provides an interface to both view the live video, and access recorded video

Waiver / Exception – Authorized deviation from this policy

Willful – Deliberate and intentional

Executive Order

Whereas: City owned and operated surveillance systems are city assets and not the sole property of any department, board, or commission.

Whereas: Federal courts including the United States, Supreme Court have repeatedly held that there is no expectation of privacy in the right of way

Whereas: The City does not believe that there should be an expectation among its citizens that they are individually and constantly subject to surveillance.

Whereas: There is an expectation of privacy on private property

Whereas: It is this philosophy that forms the basis of this Executive Order.

Section 1: Scope

1. This policy **applies** to the following:

    a. All departments, boards, and commissions that fall under the purview of the executive branch of City Government under the direct authority of the Mayor

2. This policy **does not apply** to the following

    a. Any entity that does not fall under the authority / Jurisdiction of the Mayor
    b. State and Federal Agency over which the City has no Jurisdiction
    c. Separate Elected branches of city government that do not fall under the Mayor
    d. Still images, video, audio captured to deliver specific City services including

i. Inspections
ii. Emergency services and public health responses to, and investigation of, specific emergencies and/or events.
iii. Investigations and responses to citizen complaints submitted to the Citizens Service Bureau (CSB)

3. The use of surveillance systems owned and/or operated by a third-party

Section 2: General Policy

1. The permissible and intended uses of surveillance systems are effective immediately upon the issuance of this executive order.

2. The City seeks to protect the personally identifiable information (PII) of its citizens as defined in this policy. Thus, under no circumstances shall the City use surveillance systems to target a specific individual or group unless specifically authorized as a permissible use under Table 1 of this policy.

3. The City shall not allow a third party to use a City owned and operated surveillance system or data collected to target a specific individual or group accept as accounted for in this policy.

4. The Board of Aldermen shall be notified of any substantive changes to this privacy policy and any substantive changes must be approved by the Mayor. The maintenance of this policy including change management shall be the responsibility of the Chief Technology Officer or other Mayoral Designee. Non-substantive changes shall not require approval by the Mayor or external notifications; however, published versions of this policy must include any and all changes.

5. Any Department, Board, or Commission authorized to use surveillance technologies /systems must justify their use using clear metrics and KPIs approved by the Mayor or her/his designee. Metrics and KPIs must support data driven determinations as to whether the use of these systems is having a positive impact on the intended uses called out in this policy. Authorized organizations must collect the data specified and submit an annual report to the Mayor detailing (based on the data) how their use of surveillance technologies is or is not having a positive impact. The Mayor shall, at the request of the Board of Aldermen provide these reports to the Board. Future investment decisions shall be justified based on impact. The Mayor or his/her designee shall compile and submit a bi-annual report on the use and effectiveness of surveillance technology throughout the City and make the report available to the general public.

6. The current version of this policy shall be published on the City's website. Links to the published policy shall appear on the Mayor's website and any other website belonging to a Department, Board, or Commission authorized to use surveillance technology/systems. Data regarding the use and effectiveness of surveillance

Commented [JC1]: What about this? It is dangling with nothing it refers to. If this should actually fall under 2, (which makes logical sense) then Persistent Surveillance is exempt (?) This also seems to make confusing later provisions that third parties need to be in compliance with this policy. How can you not be compliant with a policy that says you are exempt?

Formatted: Highlight

Formatted: Highlight

Commented [JC2]: But what about others? Sounds like others do not fall under Table 1.

Formatted: Highlight

Commented [JC3]: What is accounted for if they are not a city entity?

Formatted: Highlight

Commented [JC4]: Designed to make BB 94 less needed, but much less specific and totally in the hands of the mayor.

systems in relationship to permissible and intended use set forth in this policy shall be made available through the City's open data portal unless the information would compromise the security or operation of the surveillance technology/system.

Commented [JC5]: Too big and frequently misused loophole

7. **Table 1. Permissible and Intended Use**

Intended Use	Permissible Use	Policy	Conditions
Public safety	• Detection of crime • Deterrence of crime and informing measures/activities intended to reduce crime • Criminal investigations • Criminal prosecutions	• The City may continuously use surveillance systems which may include the use of biometrics and license plate readers	• Specific individuals and groups may only be targeted in conjunction with an active criminal investigation wherein the individual or group are a person/s of interest or suspect • Only for the duration of the investigation or the length of time that the person/s or groups are a person/s of interest or a suspect. • Individuals and groups may not be targeted, and any biometric data must be destroyed once they are no longer a person/s of interest or a suspect regardless of whether an investigation is concluded unless required by law.

Commented [JC6]: Applies to the City only, according to the provision above that cites Table 1.

Commented [JC7]: But doesn't apply to other (federal) agencies or private companies. They could target, or sell data or…

Commented [JC8]: Without a warrant, which is not acceptable

Commented [JC9]: But could data be used for other purposes?

Intended Use	Permissible Use	Policy	Conditions
Traffic Management	• Detection and monitoring of traffic including but not limited to vehicle, pedestrian, or other mode of transportation presence, speed, volume • Collision detection • Traffic signal optimization based on current or historic traffic patterns • Traffic signal optimization based on current traffic conditions	The City may continuously use surveillance systems	Only as it relates to traffic management and optimization
Maintenance of Right-of-Way	• Detection of unsafe conditions in the right of way (for example snow and ice accumulations, standing water) • Detection of damage to objects in the right-of-way (for example downed poles) • Detection of potential hazards and obstructions in the right-of way (for example suspicious packages, potholes, cracks in pavement, uneven surfaces, holes in sidewalks)	The City may continuously use surveillance systems	Only as it relates to maintaining the right-of-way in good working order and condition

Commented [JC7]: But doesn't apply to other (federal) agencies or private companies. They could target, or sell data or…

Intended Use	Permissible Use	Policy	Conditions
Maintenance of Public Lands	• Detection of unsafe conditions on public land (for example snow and ice accumulations, standing water) • Detection of damage to objects on public land (for example graffiti, vandalism, illegal dumping) • Detection of unauthorized or criminal activity on public land (for example theft, open air drug markets)	The City may continuously use surveillance systems	Only as it relates to maintaining public land and life, safety, asset protection on public land
Monitoring of Vacant Properties	• Protect vacant properties • Protect individuals entering unsafe vacant properties • Detect, deter, and prosecute crimes committed on vacant or problem properties	• The City may continuously use surveillance systems.	• Only for the time the property is vacant • Only for the time the property is determined to be a problem property.
Security of Public Buildings	• Safety, life, and asset protection in and immediately adjacent to public buildings	• The City may use surveillance systems to protect the safety, lives, and assets of the City, City Employees, and visitors within and in the immediate vicinity of public buildings	

Commented [JC7]: But doesn't apply to other (federal) agencies or private companies. They could target, or sell data or…

Intended Use	Permissible Use	Policy	Conditions
Public Health and Vulnerable Populations	• Find and assist vulnerable populations	• At the sole direction of the Director of the Health Department or Department of Human Services and • in response to an emergency or • when life threatening conditions exist • the Health Department and/or Department of Human Services may use surveillance systems to locate and identify vulnerable populations • for the sole purpose of rendering/providing direct assistance.	• Only in the event of an impending or existing emergency • Only for the duration of time that life threatening conditions exist • Only to detect the presence of vulnerable individuals and NOT to identify or track specific individuals
Registered Individuals	• Detect individuals who by law are not allowed to be in a certain area/s	• The City may use surveillance systems to detect the presence of individuals who by law are forbidden to be in a specific area/s. • Including the collection and use of biometrics to aid in detection.	• Only for the duration of time that an individual is forbidden to be in the area/s. • Biometrics may only be used for the duration of time the individual is forbidden to be in the area/s after which all biometric data must be destroyed. • Only in the restricted area/s.

Commented [JC7]: But doesn't apply to other (federal) agencies or private companies. They could target, or sell data or…

Commented [JC11]: What about all the data collected on others "inadvertently"?

Commented [JC10]: So, use of biometrics near schools, parks etc

Commented [JC12]: This table drops the protection against biased use against protected classes that is in the current policy; also drops the prohibition against using surveillance in private areas; drops prohibition of pan, tilt and zoom to focus on individual or use facial recognition unless there is reasonable suspicion; drops the written explanation of why policy is suspended due to imminent threats;

8. Table 2. Information Sharing and Release of Information

Third Party	We Share	Conditions
• External Law Enforcement Agencies • Recognized external security organizations (for example campus police departments, public transportation security) Note: this does not include private security firms • External entities associated with a criminal prosecution	• Current and historical video data • Biometric data • Data derived from the use of video footage and biometrics	• In conjunction with an active criminal investigation • In conjunction with a criminal prosecution • As required by law • As required by a court order
• External Public Health Organizations	• Current Real-Time video feeds • Data derived from historical video feeds	• Only with authorized third parties • Excludes biometric data
• Third parties associated with a civil case or proceeding	• We don't share	• Unless required by a warrant, or subpoena
• External Emergency Response Organizations	• We Share	• Only for the duration of an emergency • Excludes biometric data
• The general public	• Current Real-time video footage from traffic cameras at the sole discretion of the City	• We don't share any other current or historical data containing PII except as required by law

Commented [JC13]: Major change in policy; this required Appointing Authority approval before

Commented [JC14]: Is this how Persistent Surveillance {P S) gets in?

Commented [JC15]: Not in line with their accountability rhetoric regarding holding police accountable

Commented [JC16]: Again, not in line with their accountability rhetoric. This says they can't release data of police shootings, for example.

Commented [JC17]: Nothing in this Table explicitly prohibiting sharing with non-authorized users, as is in current policy.

Section 3: Systems Access, Installation, Support, Maintenance, and Administration

1. Network System Administration, System Monitoring: As this executive order will require changes to the responsibilities for system administration and monitoring, this section shall be implemented within 18 months of the effective date of this executive order.

2. The Information Technology Services Administration (ITSA) shall be responsible for the network administration, and network/fiber/switch system monitoring, of surveillance systems owned and operated by the City. This does not include federated systems not owned and/or operated by the City. While ITSA bears primary responsibility, ITSA may share these responsibilities with other City information technology (IT) departments. However, at no time shall an end user be allowed to administer, monitor, and/or audit the system to which they have been granted access. Furthermore, at no time shall a system administrator become an end user of a system he or she administers.

3. Any Department, Board, or Commission authorized to use surveillance technologies by the Mayor must keep on file, with ITSA, a list of department/board/commission heads who are authorized to submit requests for new user access to the camera software (including camera feeds) (or to remove/change user access)

4. Access to surveillance systems shall be granted to any department, board, or commission with a legitimate business need as it relates to service delivery. Department, Board, or Commission level access authorization shall be granted or denied by the Mayor or her/his designee. Once access for a Department, Board, Commission is approved the head of the Department, Board, or Commission shall be responsible for approving access for end users within their organization. Department, Board, or Commission level access requests may be submitted electronically. End user access requests must be submitted in writing. An audit of authorized end users shall be conducting by each Department, Board, or Commission at least once a year. The head of each organization must validate all end users at least once a year.

5. Approved access requests along with all supporting documentation shall be forwarded to ITSA. ITSA shall be responsible for the creation and management of all end user accounts; however, the head of each organization is ultimately responsible for keeping ITSA informed of any changes in an end user's status that impacts the type or level of access. ITSA may at any time and without notice request a user audit.

6. The City may with the approval of the Mayor or her/his designee approve access to surveillance systems by external systems as long as such access is in compliance with this policy. In the event access by an external system is granted, external systems shall only be allowed access via secure network

Commented [JC18]: Why business and not public safety?

Commented [JC19]: Drops several important things from current policy—training of end users regarding their responsibilities, use of individual passwords, log system

Commented [JC20]: What does this mean? Must they abide by City restriction? This is not explicit. How can a private company be in compliance with a policy from which they are exempted and therefore nothing applies to them? Plus,only access has to be in compliance, not sharing of data.

connections and secure Web Services or APIs. All approved access requests must include the business reasons for granting the request as they related to the permissible/intended uses outlined in this policy.

7. As it relates to public safety, the City may with the approval of the Mayor and under the terms of an information sharing agreement provide view only access to data collected by surveillance systems to a third-party public safety organization. However, only in compliance with this policy.

8. As it relates to Public Access, the City may make live video streams from some cameras available to the general public (for example: traffic cameras).

9. Back end system administration including the city owned networks that support the system/s shall be the responsibility of ITSA; however, ITSA may share or delegate these responsibilities with other City IT departments (for example: Police IT). The streets department in conjunction with ITSA shall be responsible for the installation and maintenance of City owned and operated edge devices such as cameras deployed in the right-of-way. However, the Streets Department or the Board of Public Service may use contractors to install and maintain edge devices. The edge devices are owned by the purchasing agency and not owned/maintained by ITSA.

10. All surveillance systems owned and operated by the City, shall be afforded the same cybersecurity protections as all other City systems that include sensitive information. Surveillance systems shall be included in all cybersecurity plans and solutions.

11. The City shall retain surveillance data collected for 30 days. However, at the discretion of the Director of Public Safety the City may retain data collected by all or a subset of devices for 90 days under the following conditions:

    a. The data covers an area where there is a high rate of crime.
    b. The data covers an area where the same crime/s continuously occur.
    c. The data covers an area where there is a reasonable suspicion that crimes are being committed by the same perpetrator/s.

12. Biometric data shall only be retained for the minimum period of time based on the intended/permissible use of the data.

Section 5: Policy Enforcement

1. Waivers: If in the opinion of the Director of Public Safety, or City Operations director and based on justification a deviation from the permissible and intended use or a condition as listed in Table 1 is required then the Director of Public Safety or City Operations Director may issue a temporary exception / waiver. However, justification must be based on the life, safety, or asset protection of the City and/or general public. If the deviation will be required for

Commented [JC21]: Does not say "in compliance"; again, this is only about access, not sharing

Formatted: Highlight

Commented [JC22]: Again, vague. Do third parties have to abide by City restrictions?

Commented [JC23]: But what about the systems to which data is shared? No requirement for them to have secure systems.

Commented [JC24]: This could be the whole city. And what is a "high rate"?

Commented [JC25]: None of this covers data that needs to be preserved for longer than 90 days for prosecution purposes, or for evidence in a Civilian Oversight Board complaint. All this would have to be destroyed after 90 days. Also makes no reference to compliance with Sunshine Law as is in current policy.

Commented [JC26]: What does this mean?

more than 30 days, the deviation must be approved by the Mayor and incorporated into this policy as a material substantive change.

2. Willful unauthorized access and willful abuse: Any user that willfully gains unauthorized access or abuses a surveillance system (through their deliberate action or inaction) shall be subject to disciplinary action which may include termination of employment or other relationship to the City. Unauthorized access or willful abuse shall be reported to the Mayor or her/his designee and documented immediately. Documentation shall include the nature of the incident/s and any corrective action taken.

Commented [JC27]: Is this how P S gets in?

Commented [JC28]: The current policy requires reporting to police for possible investigation, and requires immediate suspension from access if a good faith complaint is filed against someone. Current policy also has whistleblower protection and reporting requirement.