City of San José

Data Usage Protocol (DUP) for Public Security Cameras

Owning department(s): San José Police Department (SJPD)
Department owner: Intelligence Unit Commander

1) Purpose

Public security cameras are used by the Police Department to record video in public spaces where there is a known risk of criminal activity (e.g., public parks with recent vandalism, vacant public land with reports of violent activity, etc.). Since placing investigative personnel on site at all times is not practical, public security cameras are installed to both deter inappropriate use of the area as well as to document any criminal activity. This Data Usage Protocol (DUP) defines for the City of San José's (hereafter referred to as "City") Police Department ("hereafter referred to as "Department"):

1. Authorized usage of public security camera technology that complies with State and local laws;
2. Annual reporting requirements on public security camera usage; and
3. An ongoing avenue for public feedback on public security camera usage.

2) Authorized Uses:

Public security cameras shall only be used for the purposes outlined below. Any other usage by the Department or by a third party is prohibited. Third parties may only use the data if authorized by the City to act on behalf of the City. The Department and authorized third parties may utilize public security cameras and any data generated to do the following:

1. Deter criminal activity;
2. Review public security camera footage following an incident or during the course of an investigation;
3. Monitoring the safety and security of City facilities and City vehicles; or
4. Protect infrastructure installed by the City and other critical infrastructure as defined by California Office of Emergency Services (Cal OES).[1]

[1] From California Office of Emergency Services: "Critical infrastructure is the assets, systems, and networks, whether physical or virtual, so vital to the California that their incapacitation or destruction would have a debilitating effect on security, economic security, public health or safety, or any combination of these." Some examples of critical infrastructure include schools, hospitals, voting centers, community centers, and utility facilities vital to providing service (e.g., electricity, water).
Definition from Cal OES: https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/state-threat-assessment-center/critical-infrastructure-protection/
Non-exhaustive list of critical infrastructure: https://www.pacificpower.net/outages-safety/wildfire-safety/critical-facilities-infrastructure.html

3) Prohibited Uses:

Public security cameras will not be used for the following purposes:

1. Actively monitor or review security camera footage without relevance to a specific incident or investigation;
2. Collect data that is not within the public view. This includes any data not readily visible from a public area or public property;
3. Identify individuals or groups engaging in activities legally allowed in the State of California and/or protected by the First Amendment to the United States Constitution absent an incident or investigation;
4. Share with federal immigration authorities or use in the investigation of any matter related to immigration status of an individual; or
5. Sale of camera-generated data to any entity.

4) Data Collection

Public security cameras record video of public spaces of interest. The cameras may capture video of individuals and their physical likeness. Public security cameras may also record audio.

Public security cameras are placed in a fixed location, such as on a street light pole. Data collected also includes the date, time, and location of the video recording.

5) Notice

Notice that the City of San José is using public security cameras will be posted on the City website in a press release. The press release will detail the camera's location, when the camera is installed, and, if applicable, when it will be taken down (e.g., after completion of the investigation). Readers will also be directed to this Data Usage Protocol which will be available on the City website.

6) Retention and Minimization

Data collected from public security cameras will be retained for a time period consistent with the City's retention policies.[2] Once the retention period has expired, the record shall be purged entirely from all active and backup systems unless the data is related to a criminal investigation.

Data associated with a criminal investigation may be stored for longer in accordance with applicable state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations.

[2] As of last update to this document, that is one year. Refer to the City retention schedule for up-to-date information: https://www.sanjoseca.gov/your-government/departments-offices/office-of-the-city-manager/official-city-records/records-retention-schedule

7) Access and Accuracy

Except for audits, only authorized personnel, meaning Department personnel with a legitimate need and right to access the information, shall be allowed access to public security camera data.

Raw security camera data, including video, location, and timestamp will not be available for public access unless required pursuant to city, state, or federal law, or a court order. Some information may be redacted prior to public disclosure pursuant to state and federal regulations.

Aggregated data on the public security camera program will be made available annually in the Annual Data Usage Report. More details on the Annual Data Usage Report can be found in the "Annual Data Usage Report requirements" section below. The City may release more aggregated data periodically at its discretion.

8) Accountability

All Department members who use or access information from public security cameras shall be accountable for knowledge of this protocol.

Periodic, random audits may be conducted at the direction of the Chief of Police or their designee to ensure and evaluate compliance with system requirements and with the provisions of this protocol and applicable law. Audit trails shall be maintained by the Department for the time period consistent with the City's retention policy. Additional audits or reviews may be triggered at the direction of the Office of the City Manager or Digital Privacy Officer (DPO), consistent with state law and authorized access to information.

The results of the audits are subject to the law and potential California Public Records Act requests. Some information may be redacted prior to public disclosure pursuant to state and federal regulations.

Before a Department member accesses or provides access to a public security camera, the Department member shall create a record that includes the following information:

1. Date/Time the camera was provided or acquired;
2. The event number or relevant case number of the investigation; and
3. The name, department, and badge or employee number of the person who acquired or returned the camera

9) Sharing

The City does not share public security camera data with any contracted, commercial, or private entity. The provision of data hosting shall not be considered the sale, sharing, or transferring of public security camera information.

Information gathered or collected, and records retained by the City will not be:

1. Sold, published, exchanged, or disclosed for commercial purposes;
2. Disclosed or published by an entity outside of the Department without Department approval; or

3. Disseminated to persons not authorized to access or use the information.

The City shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information unless otherwise required by law. The City may agree to share access to its public security camera database by law enforcement agencies within the State of California on an agency-by-agency basis. Law enforcement agencies provided data from the Department will not share with federal immigration authorities or use in the investigation of any matter related to immigration status of an individual.

The data will not be shared beyond the approved agencies. All agencies must request SJPD public security camera data directly from SJPD (e.g., if SJPD shares public security camera data with Santa Clara PD, Sunnyvale PD must request SJPD data through SJPD rather than Santa Clara). The requesting agency may only access the data for an authorized purpose as noted in this protocol.

A log will be generated every time an outside agency is provided access to data from SJPD's public security camera system, which will include:

1. Date/Time the information was requested;
2. The event number or case number of the investigation, if no case number is available, then the purpose of requesting the data; and
3. The name and agency of the person who requested the information

10) Equity and Community Engagement

The City will make a reasonable effort to identify and mitigate any inequity inherent in public security cameras and its implementation. Members of the public may submit any concerns via the public comment feature at sanjoseca.gov/digitalprivacy. Comments may also be submitted by emailing digitalprivacy@sanjoseca.gov or mailing the Digital Privacy Officer at 200 E Santa Clara St. San Jose CA 95113, 11th Floor. Public security camera implementations can impact certain populations more than others. The City of San Jose is cognizant of that concern and will field potential complaints when submitted by emailing: digitalprivacy@sanjoseca.gov. After receiving a complaint, the City will perform an investigation and determine a corrective action plan, if necessary.

11) Storage and Security

Data collected by public security cameras shall be stored securely by police or through a third-party hosting environment. With the exception of audits, access to the raw data (video and audio recording) shall be limited to law enforcement staff with a legitimate need and right to access the information. The Department will utilize reasonable physical, technological, administrative, procedural, and personnel security measures to prevent unauthorized access to public security camera data. Authorized sworn personnel or authorized civilian personnel (such as a crime analyst) shall have general user access to the SJPD public security camera database, as appropriate, to query information. Entities authorized to audit the public security camera system (see "Accountability" section for who can authorize) do not need to be a part of the Department to access the database.

In the event of a confirmed data breach where personal information such as video recordings of identifiable individuals have been accessed by an unauthorized party, the Department will follow the City of San José's Information Technology Incident Response Plan.[3] This security protocol and further security details are overseen by the City's Cybersecurity Office.

12) Training

Department members who use public security cameras will be trained in how to:

1. Install a camera with the appropriate notice (if they are responsible for any part of the installation);
2. Securely access the information collected;
3. Document access to the information for the sake of maintaining an auditable trail of access pursuant to the "Accountability" section of this document; and
4. Adhere to current Department Data Usage Protocol regarding authorized use of public security camera technology.

13) Annual Data Usage Report requirements

To provide the City and the public with ongoing reporting on the usage and accuracy of the public security cameras, the following information will be required in an Annual Data Usage Report submitted every year to the Digital Privacy Officer (DPO) no later than March 1st and covers the previous calendar year (January 1st – December 31st). In the year this Data Usage Protocol goes into effect, the Department is only required to report on the period from the date the Data Usage Protocol goes into effect until the end of the calendar year.[4] The Digital Privacy Officer will release the report to the public once private, confidential, and otherwise sensitive information is removed. The DPO shall release the report within 90 days of receiving it from the department, unless additional time is required to remove private, confidential, and sensitive information. If the DPO needs additional time, they shall provide a notice of extension to the public via the Digital Privacy webpage.[5]

1. Reporting metrics on public security camera usage and accuracy including:
    a. **# of cameras installed, by location and duration** – the Department will report on the number of cameras installed at each location and for how long
    b. **# of records accessed by SJPD** – the Department will report on the aggregate number of usages in accordance with the Accountability section of this Protocol.

[3] An overview of Information Technology's Incident Response plan can be found in the City's Information Security Standards Handbook Section 8.7, "Incident Response": https://www.sanjoseca.gov/home/showdocument?id=85853#page=32

[4] If this Data Usage Protocol is passed after September 30th, the first Annual Data Usage Report will not be required until the following year, which will cover usage from the date the Data Usage Protocol goes into effect to December 31st of the following year

[5] Link to the digital privacy webpage: https://www.sanjoseca.gov/your-government/departments-offices/information-technology/digital-privacy