Surveillance Technology Policy

Spotery Application used for tennis reservations
Recreation and Parks Department

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of Spotery - web application used for tennis reservations itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Department's mission is to provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well- being of our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Spotery - web application used for tennis reservations will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Spotery - web application used for tennis reservations, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of Spotery - web application used for tennis reservations technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– Confirm that the person who reserved the booking for a tennis court is at the location at the reserved time.
– Utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time. Data can be accessed on the web application or as a report delivered by Spotery

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

Spotery - web application used for tennis reservations supports the Department's mission and provides important operational value in the following ways:

The surveillance technology allows for equitable access to our recreational sites.

In addition, Spotery - web application used for tennis reservations promises to benefit residents in the following ways:

X Health - Residents are able to book reservations for tennis courts which allow for recreational and physical activity.

Spotery - web application used for tennis reservations will benefit the department in the following ways:

X Time Savings, Staff do not need to review and research anecdotal evidence about reservation holders not utilizing the court for the reserved time.

To achieve its intended purpose, Spotery - web application used for tennis reservations (hereinafter referred to as "surveillance technology") allows a reservation holder to book a tennis court up to seven days in advance. 24 hours prior to the reservation, a reminder email is sent to the reservation holder. The reminder email contains a check-in button. The reservation holder can use the check-in button within 15 minutes before or after the reservation time. Spotery checks the location of the reservation holder to ensure that they are within 0.1 miles of the tennis court. Spotery needs access to the reservation holder's location so "Enable Location Services" must be turned on.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- Types of Data Collected: Name, email address, address, GPS Location (at time of check in)
- Data Classification Level: Level 2

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

- Contact information
- Data Retention
- Description of the authorized use
- Information on the surveillance technology
- Type of data collected

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Prior to accessing or using data, authorized individuals receive informal training and instruction regarding authorized uses. Informal training includes how to login and run reports.

Data must always be scrubbed of PII as stated above prior to public use.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology:

- Chief Information Officer (0941)
- Director of Property, Permits, and Reservation (0953) or designee – Administrative Analyst(s) (1820 series)

B. Members of the public, including criminal defendants

The Recreation and Parks Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Anyone, including criminal defendants, may access such data. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants.

Members of the public, including criminal defendants, may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

The access is limited only to the following roles: Chief Information Officer, Director of Property, Permits and Reservations, or designee.

Data Sharing: The Recreation and Parks Department will endeavor to ensure that other agencies or departments that may receive data collected by the Recreation and Parks Department's Spotery App Policy will act in conformity with this Policy.

For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

The Recreation and Parks Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security)

The Recreation and Parks Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their response.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- X Confirm the purpose of the data sharing aligns with the department's mission.
- X Consider alternative methods other than sharing data that can accomplish the same purpose.
- X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- X Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Recreation and Parks Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

The Chief Information Officer and the Director of Property, Permits and Reservations or designee will be responsible for enforcing the Surveillance Technology policy through recurring review of functionality and use..

The department does not share surveillance technology data externally with entities outside the City and County of San Francisco.

Before data sharing with any recipient, the Department will use the following procedure to ensure appropriate data protections are in place: Confirm the purpose of the data sharing aligns with the department's mission.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

The Department's data retention period and justification are as follows:

Retention Period	**Retention Justification**
There are two types of data collected: (a) Webapp - data on the webapp will be retained perpetually. (b) Reports - these are manually downloaded from the web app by RPD staff and are saved on the file server. These will be stored for up to 1 year.	Webapp - standard practice for commercial marketplaces. Reports - This retention period allows for ample time for staff to analyze data regarding reservation holder usage and can determine if there were any violations to RPD policy.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

- Webapp - The data on the webapp will be retained perpetually
- Reports – none

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data will be stored in the following location:

- DT Data Center
- Software as a Service Product

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Practices:

- There are two types of data collected:
    - Webapp - data on the webapp will be retained perpetually.

- Reports - these are manually downloaded from the web app by RPD staff and are saved on the file server. These will be stored for up to 1 year and deleted in an automated process.

Processes and Applications:

- At the time of check in, no PII is sent. When data is reviewed, PII data is available as this is needed for operational purposes.

Training: To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

Training is required for authorized individuals to use or access the information collected. Prior to accessing or using data, authorized individuals receive informal training and instruction regarding authorized uses. Informal training includes how to login and run reports.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Chief Information Officer and the Director of Property, Permits and Reservations or designee will be responsible for enforcing the Surveillance Technology policy through recurring review to ensure data is used only for the approved use cases: (a) Confirmation that the person who reserved the booking for a tennis court is at the location at the reserved time; (b) Utilization of data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time. Data can be accessed on the web application or as a report delivered by Spotery .

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties:

Chief Information Officer (0941) and the Director of Property, Permits and Reservation (0953) or designee - Administrative Analysts (1820 series)

Sanctions for violations of this Policy include the following:

Violation of the policy will be subject to standard RecPark departmental policies, which may include disciplinary action up to and including termination.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

DEFINITIONS

Personally Identifiable Information:	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.
Raw Data:	Information collected by a surveillance technology that has <u>not</u> been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	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.

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "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."

QUESTIONS & CONCERNS

Public:

Complaints or concerns can be submitted to the Department by:

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks through several ways: (a) Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117; (b) Call to the RPD Front Desk 415-831-2700; (c) Send an email to rpdinfo@sfgov.org; or (d) Contact 311.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall:

All calls/complaints from the public received via mail or via call to the RPD Front Desk are routed to the RPD IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the RPD IT HelpDesk which then is logged in the request management. Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion. Review of open / closed requests occur with the CIO on a weekly basis.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.