City and County of San Francisco
San Francisco International Airport

Virtual Vehicle Queuing System Technology (TNCvq)

March 19, 2026

Annie Chung, Dushyant Singh & Guy Clarke

Technology Description - TNCvq

- The primary function for the *Virtual Vehicle Queuing system (specifically, the Transportation Network Company Virtual Queue (TNCvq))* technology is using software (from QTrac and Airport developed) to provide the Airport with a text message–based virtual queue system to manage TNC staging lot demand and ensure fair access to SFO's limited staging lot space.
- The system allows TNC drivers to request entry remotely via a web browser, eliminating the need to physically approach the staging lots to check for available space. When a spot opens, drivers receive an SMS notification and may proceed to the lot for verification.
- The primary objectives of the TNCvq technology are to:

    1. Reduce roadway congestion by eliminating unauthorized/illegal staging on nearby roadways, while minimizing violations and improving safety.

    2. Streamline TNC operations and improve operational efficiency, by aiming to reduce driver conflicts and citations.

    3. Free up valuable Airport real estate for revenue-generating uses. Specifically, supporting the reclamation of Staging Lot 3 space for revenue-generating public parking usage.

TNCvq Technology – How It Works

1. As part of the TNCvq, SFO seeks to acquire software (from QTrac) - a dedicated driver registration portal, to support secure and efficient management of TNC operations.
2. Drivers are required to submit key information, including: full legal name, selfie photo, license plate number, vehicle make, model, and color, TNC profile screenshot, TNC Placard information, phone number, and email address—through this portal.
3. This information is used to manually verify each driver's identity and affiliation with an authorized TNC, match vehicles to registered users, and enable real-time communication via SMS.
4. The collected data consists of the TNC driver's commercial driving activity while operating within the Airport's geo-fence. This does not include any personal driving activity. No passenger information is collected.

TNCvq Technology – How It Works (con't)

5. The registration portal is a critical component of the VQ system, supporting accurate queue management, reducing unauthorized access to staging lots, and strengthening SFO's enforcement and auditing capabilities.
6. All data collected or processed by the TNCvq technology is handled or stored by Amazon Web Services to host the application and its data which enables the Airport to access and receive the data at any time.
7. The collected data allows SFO to monitor dwell time within the staging lots and issue citations for violations of TNC permit terms and Airport Rules and Regulations, helping to ensure fair access and efficient lot turnover.
8. SFO maintains all the data for historical analysis.

NOTE: In the Fall of 2025, SFO received Patent approval from the U.S. Patents Office for the *Virtual Vehicle Queuing system.*

Authorized Use Cases

Airport Specific Use Cases include:

- The primary function of the Virtual Vehicle Queuing system (TNCvq) is to provide the Airport with an SMS- and web-based virtual queue, using QTrac software and Airport-developed tools, to manage demand for TNC staging lots.
- Improve safety and traffic flow on Airport roadways by reducing physical vehicle queues, illegal staging, and circulation near the staging areas.
- Monitor Transportation Network Company (TNC) driver compliance with their Operating Permit conditions and Airport Rules and Regulations, including identifying violations and enabling suspensions, prohibitions, and citations when necessary.
- Collect, process, and retain operational data, including TNC driver Personally Identifying Information (PII), as part of the ground transportation management, analytics, auditing, and reporting process.
- Ensure that only authorized and approved drivers and vehicles are permitted to operate at SFO by verifying identities, vehicle information, and valid TNC affiliations through a dedicated registration portal.

Data Lifecycle: Data Collected

Data captured is classified as Level 3, Sensitive.

This data includes:

- Full legal name (as shown on driver's license), Phone Number & Email Address
- Self-Photograph
- Screenshot of TNC (Transportation Network Company) profile screenshot & TNC Placard Information

- All data will be retained for:
  - Transportation Planning purposes
  - Enforcement of Operating Agreements
  - Regulation of Mobility Programs
  - Ensuring the Equitable Distribution of Transportation Options throughout the Airport.

Data Lifecycle: Data Deletion & Retention

1. All registered TNC drivers will have the option to request deletion of their driver profile and all associated personally identifiable information (PII) via the Driver Web Portal under the account management section.
    - Once a driver submits a deletion request, the profile will be scheduled for automatic deletion within seven (7) days. During this period, the driver may cancel the deletion request if it was submitted in error.

2. All registered and approved TNC drivers are required to accept the Terms and Conditions every twelve (12) months to remain opted in and continue operating under the TNCvq program. If a driver does not accept the Terms and Conditions within the required timeframe, their profile will be placed in inactive status, and they will not be permitted to operate at SFO.

3. The system will automatically delete all driver PII data after five (5) years if the driver profile status is anything other than active.
    - Driver trip-related data will be retained indefinitely for analytical purposes only. This data will be anonymized to ensure that no personally identifiable information (PII) is retained.

Thank You

Data Lifecycle: Data Access

1. Prior to accessing or using data, authorized individuals receive training in system access and operation, and instruction regarding authorized and prohibited uses.
2. For investigative purposes, Department access to data is restricted to specific and trained personnel. Location data that is used for prosecution or investigation purposes could be retained beyond the stipulated retention period(s).
3. For litigation purposes, the City Attorney's Office has been provided data upon request.
4. Personnel with access belong to the following groups:

- SFO Ground Transportation Unit (GTU)
- SFO IT (Ops Support)
- SFO Law Enforcement Partners
- SFO Landside Operations

Data Lifecycle: Data Security

1. Departments shall, at minimum, apply the following safeguards to protect surveillance technology information from unauthorized access, control, and misuse by using the following:
    - Password protected systems
    - Encrypted Storage
    - Physical Safeguards
    - Audits

2. Data is reviewed for Personally Identifiable Information (PII) and must always be scrubbed of PII as stated above prior to public use.

3. Access to systems utilizing wireless networks are required to be equipped with WPA2 security.

4. Written authorization from the Department is required prior to release of data.

Other Pertinent Information: TNCvq

Technology includes:

- The Technology is hosted on AWS cloud service – managed by SFO.
- All service provider systems are service-provider-owned.
- Service providers are required to provide data they manage and store to SFO in real-time.
- The Airport's on-premise systems are comprised of private cloud and on-premise hardware that ingest and store the data and process analytic reports.
- **NOTE:** SFO recently received Patent approval from the U.S. Patents Office for the *Virtual Vehicle Queuing system.*