COUNCIL AGENDA: **9/20/2022**
FILE: **22-1387**
ITEM: **3.5**

CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: HONORABLE MAYOR AND CITY COUNCIL

FROM: Khaled Tawfik
Anthony Mata

SUBJECT: **DIGITAL PRIVACY UPDATE AND PUBLIC CAMERA USE**

DATE: August 22, 2022

Approved Jennifer A. Maguire

Date 09/09/22

RECOMMENDATION

(a) Accept the status report on the progress of the Digital Privacy Program.
(b) Accept new and updated data usage protocol documents for the Transportation and Parks, Recreation and Neighborhood Services departments.
(c) Approve the Data Usage Protocol for Automated License Plate Readers to replace the Police Department's existing Data Usage Policy in Police Duty Manual L4207 and to supersede previously approved automated license plate reader related policies.

OUTCOME

City Council will provide feedback on the progress of the Digital Privacy Program and the data usage protocol documents for the Transportation and Parks, Recreation and Neighborhood Services departments, and approve the Data Usage Protocol for Automated License Plate Readers to replace the Police Department's existing Data Usage Policy in Police Duty Manual L4207 and to supersede previously approved automated license plate reader related policies. These actions will enhance public and transportation safety and provide City efficiencies.

EXECUTIVE SUMMARY

The City began to explore a programmatic approach to protecting the digital privacy needs of San José residents and visitors in 2017. After adopting its Digital Privacy Policy in 2020, the City implemented base reviews and controls in 2021, and hired a dedicated Digital Privacy Officer. The City has become one of a small number of cities leading efforts to balance the use of Smart City technologies (e.g., cameras and sensors) to improve the lives of residents, while protecting the digital privacy interests of the community.

The goal of the City's Digital Privacy program is to provide the best services to all residents possible while protecting their privacy. San José is one of the leading cities in both innovation and privacy in sensing technologies. As a result, the City has opened an ongoing dialogue with residents, privacy experts, and staff on the community benefits of new technology.

The City has pushed transparency in its technology. In response it has received a mix of critiques, expert input, and appreciation from stakeholders for engaging them in the conversation. In the last year, the City reviewed over 100 of its technology and data practices to ensure compliance with its Digital Privacy Policy, and continues to guide Smart City innovation in a manner that addresses and respects residents' privacy.

This memorandum outlines the City's privacy practices which have been informed by City's stakeholders. City practices will continue to evolve with ongoing input. Three Smart City initiatives that use cameras in ways that will improve services while protecting privacy are highlighted below:

1. San Jose Police Department's (SJPD) usage of Automated License Plate Readers for enforcement;
2. Department of Transportation's (DOT) usage of video and artificial intelligence for automated traffic data collection to improve traffic safety, flow, and operations; and
3. Department of Parks, Recreation and Neighborhood Services (PRNS) usage of video for automated people counting.

In these use cases, the departments navigated privacy concerns and developed solutions to improve necessary City services while mitigating privacy risks to ensure compliance with the City's Privacy Principles and Digital Privacy policy. In coordination with the Digital Privacy Officer, departments established the following:

1. **Minimization** and **retention**: Thoughtfulness in only collecting the necessary data to reduce costs and privacy risk while providing services;
2. **Accountability** and **Access**: Defined data usage and access limitations, ensuring the data is only used by the authorized people to support, protect, and secure our communities, and creating a process to monitor the data usage and access over time;
3. **Sharing**: Established data reporting standards to track the annual usage of the technology; and
4. **Notice** and **Equity**: Opened avenues for the public to learn about the new technology so they can understand why it is being installed, and how they can get involved.

With this approach, the City is serving as a leader for digital privacy in cities nationwide.

BACKGROUND

The City began to explore a programmatic approach to protecting the digital privacy needs of San José residents and visitors in 2017. The advance of Internet of Things technologies and the exponential growth of connected devices caused staff to recognize the potential risks that pervasive sensing data could pose to the community. Engaging the Harvard Berkman Klein Center for Internet & Society, the City concluded that:

1. Federal action and guidance on privacy would be too slow;
2. Leading states were passing different and competing privacy legislation;
3. Very few cities had made real progress on digital privacy; and
4. Privacy principles with a strong connected policy would be key as technologies outpaced caution.

Staff from the City Manager's Office of Civic Innovation and the Information Technology Department worked with the Harvard Berkman Klein Center for Internet & Society, an internal cross-department Digital Privacy Working Group, and an external Digital Privacy Taskforce[1] to define San José's path for creating a digital privacy program fitting the requirements of modern government and emerging technologies.

The Mayor and City Council approved the resulting work as the City's Digital Privacy Policy[2, 3] on December 8, 2020, and effective July 1, 2021. This established the foundation of the City's Digital Privacy Program. The Information Technology Department led immediate work to implement basic privacy review processes for major projects and purchases, defined a start-up privacy program, and developed the job description for the City's Digital Privacy Officer (DPO) to support all departments as the Citywide privacy lead.

As part of the 2021-2022 Budget process, the Mayor and City Council approved the DPO position.[4] In October 2021, the City hired the DPO and formally initiated the Digital Privacy Program and its long-term work plan. The DPO is responsible for partnering with City departments and external stakeholders to implement the City's Digital Privacy Policy, preserving community trust in how the organization collects, processes, and uses information.

Throughout the creation of the Digital Privacy Program, the City coordinated with privacy experts from its Digital Privacy Advisory Taskforce, City departments, and peer governments. This allowed the City to develop and implement a formal process for privacy reviews that weighs civic benefits against potential risks, as well as data usage controls that help manage those decisions in day-to-day City operations.

In February and March of 2022, City staff presented progress on the Digital Privacy Program to the Smart Cities and Service Improvement Committee[5] and the Public Safety, Finance, and Strategic Support Committee[6]. From these committee meetings, staff received the following feedback:

---

[1] Digital Privacy Advisory Taskforce on the Digital Privacy: https://www.sanjoseca.gov/your-government/departments-offices/information-technology/digital-privacy
[2] Digital Privacy memo and presentation from the 12/8/2020 City Council Meeting: https://sanJosé.legistar.com/View.ashx?M=F&ID=8931718&GUID=5744C552-4DED-40B8-9D1A-123DCB1CF2CC and https://sanJosé.legistar.com/View.ashx?M=F&ID=8997095&GUID=CEB58E6D-8D87-4459-AA7B-5B26F9881A4C
[3] City of San José Digital Privacy Policy: https://www.sanjoseca.gov/home/showpublisheddocument?id=68053
[4] City of San José 2021-2022 Adopted Operating Budget, Page 28: https://www.sanjoseca.gov/home/showpublisheddocument/78329/637739734655100000
[5] Item (d)3 at the February 3, 2022, Smart Cities and Service Improvement Committee meeting: https://sanjose.legistar.com/LegislationDetail.aspx?ID=5381557&GUID=6AF73AE0-79E7-453E-A365-B9D984474BBD
[6] Item (d)4 at the March 17, 2022 Public Safety, Finance, and Strategic Support Committee meeting: https://sanjose.legistar.com/LegislationDetail.aspx?ID=5466662&GUID=A9F3AFC2-FD0F-4FC6-A918-D4EEF70B802C

1. Appreciation for the privacy outreach
    a. Engagement provides transparency and peace of mind to residents
    b. Reviews ensure data is used for the community's benefits
2. Concerns around the approach to privacy
    a. Privacy reviews risk slowing down progress in the City
    b. Data usage limitations may reduce the effectiveness of efforts
3. Direction for the Digital Privacy Program
    a. Continue and expand community engagement efforts on City technology
    b. Review and update data usage policies on Automated License Plate Readers

This update reviews in detail the progress of Digital Privacy Program following Committee direction and the application of the Digital Privacy Policy to three key use cases:

1. SJPD's usage of Automated License Plate Readers (ALPR) for enforcement;
2. DOT's usage of video and artificial intelligence to improve traffic safety and flow; and
3. PRNS's usage of video for automated people counting.

ANALYSIS

SJPD: ALPRs

ALPRs use high speed cameras angled to capture images of vehicle license plates visible from public roads. The purpose of ALPR cameras is to support criminal investigations, especially vehicle-related crimes such as hit-and-runs and stolen vehicles,[7] and to provide a tool to reduce crime in a specific area.[8]

An example image captured from an ALPR camera is provided in Figure 1. While the ALPR camera is angled to capture license plate information, it may collect additional information visible in the image, including car make/model, and other distinguishing characteristics of the vehicle (e.g., bumper sticker(s), after market wheels).

ALPR cameras may be placed in a fixed location, such as on a street light pole, or in a roaming location, such as on a police vehicle (shown in Figure 1). Cameras are angled to take pictures at the height of a license plate. The technology will record the date and time the image was captured, as well as the location of the camera. The location of vehicles can be inferred based on the location of the camera at the time of the photograph.

[7] Koper, Christopher S., and Cynthia Lum. "The impacts of large-scale license plate reader deployment on criminal investigations." *Police Quarterly* 22.3 (2019): 305-329 – https://journals.sagepub.com/doi/abs/10.1177/1098611119828039

[8] Koper, Christopher S., Bruce G. Taylor, and Daniel J. Woods. "A randomized test of initial and residual deterrence from directed patrols and use of license plate readers at crime hot spots." *Journal of Experimental Criminology* 9.2 (2013): 213-244 – https://link.springer.com/article/10.1007/s11292-012-9170-z

Figure 1: Example picture from an Automated License Plate Reader Camera from the Pasadena, California Police Department. This picture identifies 1) the license plate, 2) the time and location of the car at this time, and 3) any other information captured in the photograph. Source - https://www.pasadenanow.com/main/city-council-to-consider-purchasing-more-automatic-license-plate-readers

ALPR cameras **do not** look into a person's private residence, back yard, or private property. SJPD requires a higher bar be met before recording in any private area.

For example, SJPD's Unmanned Aircraft System, or the usage of unmanned aircraft (drones) for police purposes, underwent significant public outreach and City Council input dating back to 2015.[9] From these discussions, SJPD established an operating procedure for its Unmanned Aircraft System[10] that covered:

1. Limitations on when the Unmanned Aircraft System can be used to examine private property, such as following consent from the relevant parties, a warrant, or in the event of an emergency; and
2. A record of all Unmanned Aircraft System usage, including the date, time, and location, which can be found on SJPD's website.[11]

While the City will only use ALPR in public areas, it still defines a clear usage protocol in Police Duty Manual L4207,[12] and the updated version attached to this memorandum. The City also maintains an ALPR transparency portal, which reports the usage of stationary ALPR by SJPD.[13]

[9] Advertisement for one of the community meetings held in 2015 at the Mayfair Community Center: https://nextdoor.com/agency-post/ca/san-jose/san-jose-city-council/next-meeting-on-sjpd-drone-policy-sat-feb-14-9165954/
[10] Full Unmanned Aircraft System Operational Procedure: https://www2.sjpd.org/records/pc-13650_library/Unit%20Guidelines/UAS%20Unit%20Guidelines.pdf
[11] 2019 – 2022 Unmanned Aircraft System flight log: https://www.sjpd.org/records/uas-deployments
[12] San José Police Department Duty Manual L4207; approved by Council as item 8.2 on January 24, 2017: https://www.sanjoseca.gov/home/showpublisheddocument/57582/637248116781300000
[13] San José Police Department ALPR transparency portal for stationary cameras: https://transparency.flocksafety.com/san-jose-ca-pd

The City's History with ALPR

SJPD has used ALPR technology since 2006, and developed a usage protocol for ALPR in 2017[14]. Until recently, all of SJPD's ALPR cameras have been attached to a police patrol car, providing officers a quick way to check passing vehicles. City Council approved the City's first installment of stationary ALPR on September 21, 2021, for the intersection at Monterey and Curtner in response to three unsolved hit-and-run fatalities that year, among other serious traffic incidents.[15] In November of 2021, City Council approved an additional $250,000 for ALPR camera installation in response to "smash-and-grab" thefts, vehicle thefts, and drive-by shootings.[16]

In April of 2022, the City moved forward with procurement of gunshot detection devices and corresponding ALPR cameras after receiving funding from the Urban Areas Security Initiative (US Department of Homeland Security Office for Domestic Preparedness, UASI) in the amount of $232,000 for a pilot gunshot detection/ALPR System program. City Council also made a $71,000 ongoing ask for ALPR (paired with gunshot detection) in the 2022-2023 budget.[17]

Given the introduction of stationary ALPR and overall ALPR expansion, City Council directed the City Manager to revisit ALPR usage protocols in Quarter 1 of 2022.[18] Following updates at the February 2022 Smart Cities and Service Improvement Committee meeting,[19] and the March 2022 Public Safety, Finance, and Strategic Support Committee meeting,[20] City staff, with advice from the Digital Privacy Advisory Taskforce and input from the public, created an updated Data Usage Protocol (Protocol) to support public education on ALPR.

Why it Matters

ALRPs provide a new way to support safety and accountability, but without proper restrictions, can allow an invasive view into peoples' lives. The City's approach applies controls consistent with its Privacy Principles.

2021 saw three fatal hit-and-run crashes at the intersection of Monterey and Curtner with no evidenced suspects. It is possible that the evidence from an ALPR camera could have identified the vehicles and brought justice for the families of these victims. It is possible this technology could deter future crimes and bring justice to future victims and their families.

---

[14] *Ibid*, see footnote 12
[15] Item 4.1 of the September 21, 2021, City Council Meeting: https://sanjose.legistar.com/View.ashx?M=F&ID=9792966&GUID=4344E08A-7CF9-4A78-A6E4-91A8A28CAFF3
[16] Item 3.6 of the November 30, 2021 City Council Meeting; see item 3 in the Council memo from Liccardo, Jones, Carrasco & Mahan: https://sanjose.legistar.com/View.ashx?M=F&ID=10299569&GUID=7EC34F81-EB33-4E3B-BE1B-B67AD5657882
[17] See Council Budget Document #22, "Camera/Gun Shot Detection in District 1": https://www.sanjoseca.gov/home/showpublisheddocument/86261/637891579353030000
[18] *Ibid*, see footnote 16
[19] Item (d)3 at the February 3, 2022 Smart Cities and Service Improvement Committee meeting: https://sanjose.legistar.com/LegislationDetail.aspx?ID=5381557&GUID=6AF73AE0-79E7-453E-A365-B9D984474BBD
[20] Item (d)4 at the March 17, 2022 Public Safety, Finance, and Strategic Support Committee meeting: https://sanjose.legistar.com/LegislationDetail.aspx?ID=5466662&GUID=A9F3AFC2-FD0F-4FC6-A918-D4EEF70B802C

However, we also live in a time of growing government control worldwide. We know that policing throughout the country has historically targeted black and brown communities. Blindly using technology that automates decisions and captures large amounts of data can worsen this issue. Hence, the City created privacy protections to ensure all communities can benefit from the innovative technologies in ways that are responsible and transparent.

Summary of the Privacy Review

Any City technology procurement or new initiative that law enforcement can use to help identify a suspect, like ALPR technology, is reviewed by the DPO. While the technology is designed to only capture images in public areas like public intersections, and license plates are designed to be publicly visible, the usage of ALPR was assessed as a high privacy risk given:

1. The high volume of data collected (over 750,000 images collected in 2021);
2. The direct usage by law enforcement to identify individuals for criminal charges; and
3. The lack of consent provided. ALPR cameras automatically take pictures of vehicles as they pass a public intersection, meaning individuals cannot "opt-out" of having their license plates photographed unless they actively avoid areas where the cameras are placed.

Given these privacy risks, SJPD worked with the DPO to design an updated Data Usage Protocol that provided police officers with the tools they needed to investigate and deter crime, while mitigating the loss of privacy and civil liberties. The proposed Data Usage Protocol is attached to this memorandum. Staff requests City Council take action on this Protocol, as it would replace the previous policy in Police Duty Manual L4207, approved in 2017.[21]

For City Council's determination, the key elements of this recommended Data Usage Protocol include:

1. Transparency: an auditable trail of all ALPR usage by SJPD, defined audit authority, and annual reporting requirements on the usage of ALPR in the City.
2. Controlled Data Sharing: Often, a major crime crosses jurisdictions and it is essential to coordinate with neighboring agencies. The Protocol allows SJPD to create sharing agreements with California law enforcement agencies but does not allow the City to offer federal agencies access to the data. All shared data is tracked and can be audited to identify if, when, and how other agencies are accessing ALPR data collected in San José.
3. Expectations to Provide Notice: Notice, typically in the form of signs or online information, provide transparency to the public and potentially deter vehicle crime.[22] The City will install signage in the areas where stationary ALPR is in use as a standard practice. One of the signs installed near the Monterey and Curtner intersection is shown in Figure 2.

[21] San José Police Department Duty Manual L4207; approved by City Council as item 8.2 on January 24, 2017: https://www.sanjoseca.gov/home/showpublisheddocument/57582/637248116781300000

[22] Koper, C.S., Taylor, B.G. & Woods, D.J. A randomized test of initial and residual deterrence from directed patrols and use of license plate readers at crime hot spots. *J Exp Criminol* **9,** 213–244 (2013). https://doi.org/10.1007/s11292-012-9170-z

4. Defined Purpose: Given City Council goals, SJPD needs, advice from the Privacy Advisory Taskforce, and input from the public, the Protocol sets out clear authorized uses for crime investigations, finding stolen vehicles, and Amber and Silver alerts. The Protocol also details prohibited uses, such as investigating immigration status, actively monitoring First Amendment activities, and automatically enforcing crimes like traffic violations. A full list can be found in the Data Usage Protocol.

Figure 2: Signage posted at the intersection of Monterey Road and Curtner Avenue.

Summary of Outreach

A goal of this privacy review was to inform the public on ALPR technology and how it could be used in the city. The DPO, SJPD, and City Manager's Office of Communications coordinated to speak at six in-person neighborhood association meetings regarding ALPR spanning the Foxdale, Cadillac/Winchester, Poco Way, Roundtable, Jeanne, and Guadalupe/Washington neighborhoods.

Staff chose outreach locations based on areas with high risk of traffic incidents and near major roads including the U.S. 101, I. 280/I. 680, Hwy. 17, Monterey Road, and Capitol Expressway. The City provided an online meeting on August 24, 2022, to reach residents who could not attend in-person meetings. The Citywide online meeting was advertised on social media, Nextdoor, flyers at community centers and libraries, emails to neighborhood associations, and through a media advisory.

The information sessions reached more than 300 families in-person and more through the City-wide ALPR webinar event. Additionally, informational materials were sent to residents of the five neighborhoods via email and were published online via the Digital Privacy webpage[23] for anyone to view.

[23] Digital privacy webpage: http://sanjoseca.gov/digitalprivacy

Feedback across the sessions covered the following key themes:

1. Appreciation that the City provided this information session;
2. Who can access the data (only trained SJPD staff), and how long the data will be stored (one year);
3. How the data will be used (the City received positive feedback for having defined usage);
4. Requests to put the ALPR cameras in their neighborhoods, and questions around how to request these cameras;
5. How much the stationary cameras cost (~$2,800/year for SJPD uses); and
6. Support for the usage of the technology for parking and enforcement and abandoned vehicles.

Next action for ALPR

Following review across City Attorney's Office, SJPD, the Information Technology Department, and the City Manager's Office, City staff presents the recommended ALPR Data Usage Protocol attached to this memorandum to replace the existing policy in SJPD Duty Manual section L4207 and to supersede previously approved automated license plate reader related policies, including the ALPR policies outlined in item 3.6 of the November 30, 2021, City Council meeting.[24]

DOT: Automated Traffic Data Collection

What is New for the City's Traffic Safety and Operations

In the ongoing Vision Zero[25] effort to reduce and eventually eliminate traffic deaths and severe injuries in San José, DOT is piloting a "vision based" traffic data collection system. The system uses a video camera to automatically collect traffic data, such as the number of near-collisions at an intersection, to assess the safety of the intersection before and after safety counter measures are put into place, e.g., pedestrian related signal timing, curb bulb outs, and road dividers.

[24] See item 3.6 of the November 30, 2021, City Council Meeting; see item 3 in the Council memo from Liccardo, Jones, Carrasco, and Mahan: https://sanjose.legistar.com/View.ashx?M=F&ID=10299569&GUID=7EC34F81-EB33-4E3B-BE1B-B67AD5657882

[25] Learn more about San José's Vision Zero plan online: https://www.sanjoseca.gov/your-government/departments/transportation/safety/vision-zero

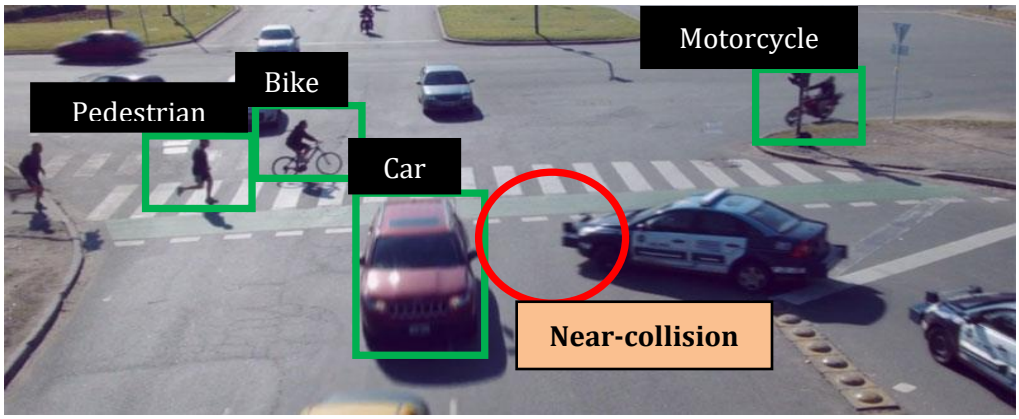

Figure 3: Example of a camera counting the vehicles, pedestrians, and near-collisions using Artificial Intelligence. This is not a picture of San José, and is only an example

Why it Matters

It is impossible to have a human monitor an intersection at all times. Cameras can continuously count the number of passing vehicles, the number of turns taken, traffic flow anomalies, and the number of safety incidents at an intersection. With this data, DOT staff can identify what improvements can increase safety at each intersection.

However, constantly recording would present the City with massive amounts of data storage costs and non-compliance with the City's Digital Privacy Policy on data minimization.[26] DOT recognized the inefficiency of collecting all possible data and instead only collect what is needed.

Summary of the Privacy Review Process and Communication with the Public

DOT only needs a fraction of the information the cameras can collect, which is why the artificial intelligence of the cameras is designed to only collect:

1. Safety incident analytics: red-light running, speeding, near misses, wrong way driving, slow and stopped traffic, jaywalking, stop sign violations, and encroachment on a double line, crosswalk, bike lane, or bus lane; and
2. Traffic operations metrics: vehicle turning movement counts, vehicle counts by classification (e.g., truck, bus, small car), pedestrian counts, bike counts, wait times, occupancy, headway, queue length, stop counts, 85th percentile speed, average speed, and arrivals on green.

The data can also be processed to determine delays or level of service,[27] which are commonly used metrics to assess congestion levels.

---

[26] From the City's Digital Privacy Policy, Data Minimization is "Minimizing the collection and processing of identifying information and limiting collection to only what is necessary to provide services and to conduct business." See the full policy here: https://www.sanjoseca.gov/home/showpublisheddocument/80514/637750765655100000

[27] Level of service refers to the level of congestion at an intersection, from free flow to bumper-to-bump traffic.

Sound is not collected, and nearly all video footage is deleted immediately. In the event of a safety incident, the system records images and video clips of approximately three seconds, so that DOT can visually verify the data collected. By storing only short clips rather than all video, DOT saves on data management costs—roughly $3,000 per camera per year on data storage alone.[28]

Some personal information may be collected incidentally, but cameras are typically located far enough away that license plates and faces are not identifiable, lowering the privacy risk (see example footage from the cameras in Figure 4). Moreover, neither the cameras nor the system was designed to identify individuals, only safety incidents like the ones outlined above.

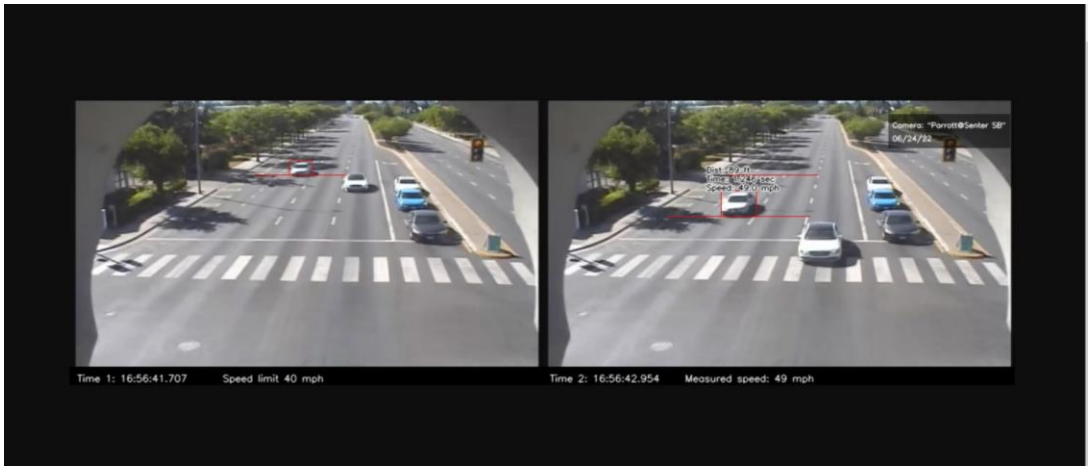

Figure 4: Two pictures from San José's traffic cameras.

DOT and the DPO collaborated on how to communicate this new technology to residents and developed three tactics:

1. Creating a Data Usage Protocol to explain what data is being collected and how it is being used. This Data Usage Protocol is available online for anyone to view.[29]
2. Installing signage upon approach at all intersections with cameras to notify residents that the technology is in use. The signage will not only notify residents, but also provide them a QR code for pedestrians to scan and an easy URL (sanjoseca.gov/digitalprivacy) to learn more about the technology.
3. Discussing the technology in future community outreach alongside other Smart City technology in San José.

[28] Perspective: A 1080p HD camera recording all day would require about 31 gigabytes (GB) of storage per day. If that data were stored for at least one year per California data retention laws (Government Code 34090), a single camera would store 11,388GB before staff could delete data. Current cloud storage costs between $0.25 to 0.3 per GB per year, or $2,847 to 3,416.40 for the 11,388GB collected in a year.
[29] See http://sanjoseca.gov/digitalprivacy for all published and draft data usage protocols

Next steps for Automated Traffic Data Collection

Following review by the City Attorney's Office, DOT, the Information Technology Department, and the City Manager's Office, City staff presents the recommended Data Usage Protocol for automated traffic cameras, available online.[30]

PRNS: Automated People Counting

What is Automated People Counting?

The City's Department of PRNS has limited resources to split between its various parks, trails, and community centers. By understanding how many people use each facility and what times of day/days of the week people attend, PRNS can better prioritize maintenance, adjust facility hours, and provide programs that best serve the community.

Traditionally, PRNS relied on a staff member counting the number of people in a facility, which requires dedicated staff time and could only sample the attendance at a point in time. In response, PRNS and Public Works are piloting automated people counting cameras at two facilities: Berryessa Community Center and Mayfair Community Center. These cameras will be able to count attendance at all times, and can provide real-time information on facility usage to optimize maintenance, hours, and program schedules.

The cameras work by counting the number of people and vehicles that cross into the cameras' fields of view. If they cross from one direction, they would be counted as entering. If they cross from the other direction, they would be counted as exiting. The pilot cameras do not store the video, only the counts of enters and exits. See Figure 5 below for an example image.

[30] Traffic video metrics Data Usage Protocol is available on the Digital privacy webpage: https://www.sanjoseca.gov/digitalprivacy; direct link here: https://www.sanjoseca.gov/home/showpublisheddocument/88839/637975454916970000

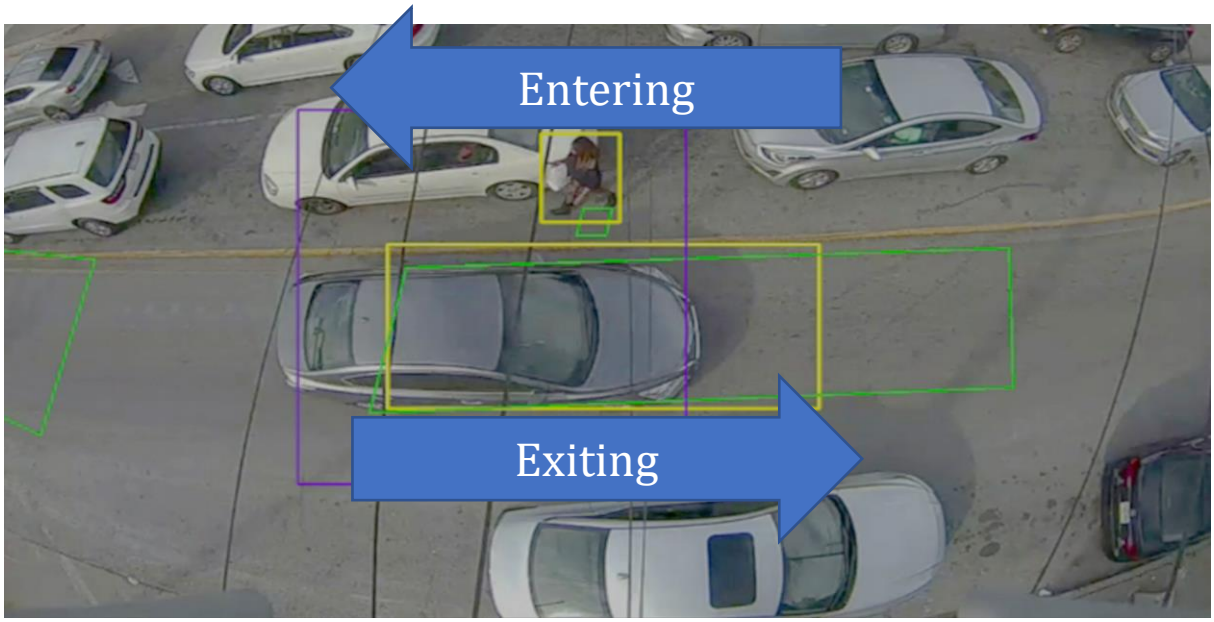

Figure 5: Example image from pilot vendor Ubicquia, showing the camera recognizing a person entering and a car exiting. This image was not taken in San José.

Why it Matters

PRNS does not have the staff capacity to manually count facility usage 24 hours a day/ seven days a week. The cameras enable PRNS to collect data on facility usage around the clock and in real time. Once the pilot cameras are installed, PRNS can better understand the traffic in its facilities, so they can optimize open hours, programming schedules, and staff presence to best meet the needs of the most residents.

Summary of the Privacy Review and Communication with the Public

Pilot cameras are set to not store the video by design, only retaining the counts of entering and exits (shown in Figure 6). No identifying information is stored, eliminating most privacy risk. The focus of this review was on clear communication with residents. PRNS and the DPO wanted to ensure curious or concerned residents could learn about the new cameras being installed, and understand how they are being used.

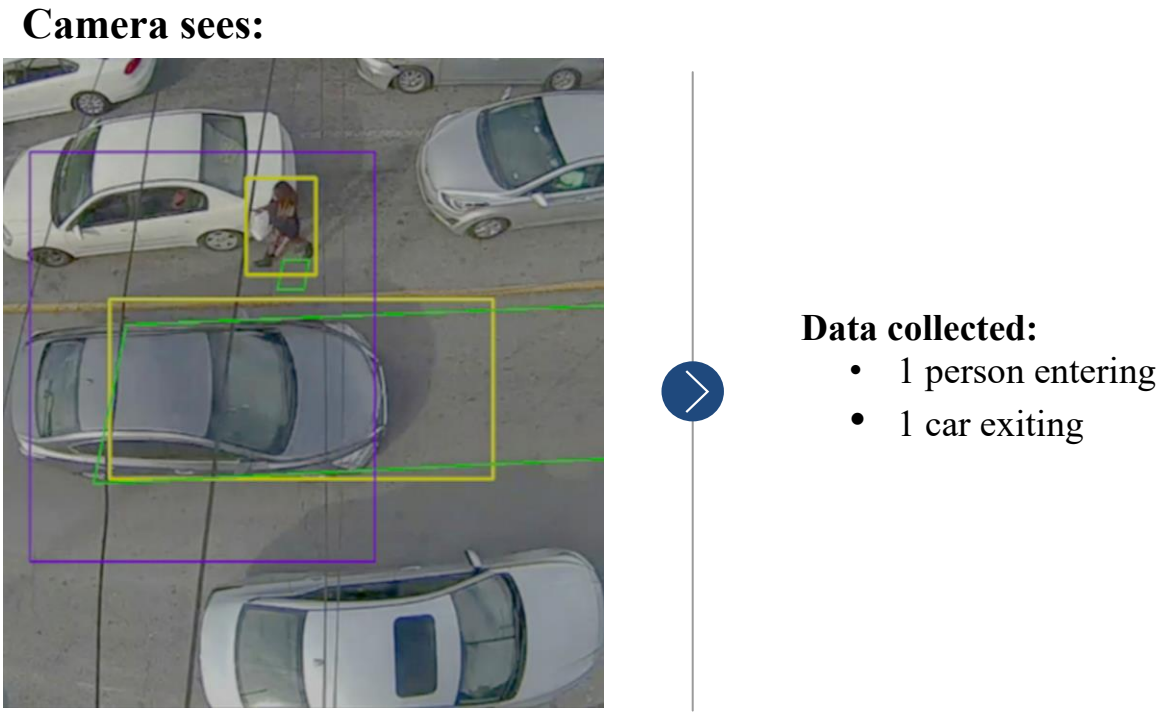

Figure 6: Example of what the camera sees and what data is collected. The data that is stored, the number of people and cars entering and exiting, does not contain any identifying information.

PRNS collaborated with the DPO, Public Works, and DOT to craft signs that will inform residents of the cameras and allow them to learn more. The proposed sign in Figure 7 informs residents of the presence of cameras across four languages. The sign includes a QR code, which takes residents to the Digital Privacy webpage[31] to learn more about the project.

[31] Digital Privacy Webpage: https://www.sanjoseca.gov/digitalprivacy

Figure 7: Sign to be posted alongside the people counting cameras. It provides the information in four languages, and provides a QR code to San José's Digital Privacy webpage to learn more

Next Steps for PRNS People Counting

Following review by the City Attorney's Office, PRNS, the Information Technology Department, and the City Manager's Office, City staff presents the recommended Data Usage Protocol for automated people counting cameras, available online.[32]

PRNS will measure the accuracy and value of the data generated by the automated people-counter cameras, and determine if it is worth expanding to other parks, trails, and community centers.

CONCLUSION

Since City Council adopted the City's Digital Privacy Policy, the City has served as a leader in using technology to improve the lives of residents while protecting their privacy.

The City's approach is to (1) take care in its uses of sensing technologies and related data and (2) engage in an ongoing dialogue with community stakeholders, privacy experts, and staff to make responsible decisions as sentiments evolve. The City has received a variety of fair critiques, expert input, and appreciation from residents for its approach. The transparency of City efforts will continue to fuel the dialogue. As the City continues to engage its stakeholders on privacy

[32] PRNS People Counting Data Usage Protocol is available on the Digital privacy webpage: https://www.sanjoseca.gov/digitalprivacy; direct link here: https://www.sanjoseca.gov/home/showpublisheddocument/87366/637914980388000000

matters, the City's privacy practices, protocols, and processes will refine and improve over time. Progress to date for the Digital Privacy Program can be summarized in four main points:

1. Thoughtful feedback from City Council, community organizations, City staff, Privacy Taskforce experts, members of the public, and outside governments. This input informs the City's direction in privacy, and has been met with an appreciation for the City's efforts at engagement.
2. Progress in San José's Drive to Digital and all services using data following the hiring of the DPO who developed and put into practice leading privacy processes for review, public engagement, and data usage policies.
3. Implementation of privacy reviews in over 100 projects. The Digital Privacy Program will continue to evolve as needed with the support of the City's Digital Privacy Advisory Taskforce, peer government partnerships, and feedback from the public and City staff.
4. National leadership in government digital privacy, sharing the City's practices with other jurisdictions and learning from peers through national privacy forums like the Center for Digital Government, Institute of Electrical and Electronics Engineers and the Future Privacy Forum.

City departments continue to collaborate to make progress towards San José's "Digital Equity" and "Drive to Digital" priorities. By continuing to engage the public, City staff and external privacy leaders, the City is defining clear, responsible data usage for a smarter, more equitable San José.

EVALUATION AND FOLLOW-UP

The Information Technology Department will report progress on Data Usage Protocols and overall progress on the City's Digital Privacy Program at future committee and City Council meetings when milestones occur or as requested.

Key next steps include:

1. Continue drafting and engaging the public on Data Usage Protocols for upcoming and existing priority data initiatives to align with the City's Digital Privacy Policy.
2. Expand the City's equity through data and privacy efforts with support from the Information Technology Department, City Manager's Office, and the Knight Foundation.
3. Continue to develop the City's Digital Privacy Program model to help lead national adoption of digital privacy programs in state and local governments, and building a community of practice on digital privacy.
4. Grow the Digital Privacy Advisory Taskforce as the City conversation on privacy transitions from privacy principles to applying digital privacy to City priorities.
5. Continue to build an internal community of practice among City staff through the Digital Privacy Working Group.

CLIMATE SMART SAN JOSÉ

The recommendation in this memorandum has no effect on Climate Smart San José energy, water, or mobility goals.

COMMISSION RECOMMENDATION/INPUT

This report was not presented at a commission meeting.

PUBLIC OUTREACH

This memorandum will be posted on the City Council agenda website for the September 20, 2022 City Council meeting. In addition, the City has coordinated with the Digital Privacy Advisory Taskforce (reviewed June – August 2022) and has engaged the community on traffic sensing technologies through in-person and online events. The City will continue to engage residents in person, online, and via signage placed near the technology.

COORDINATION

This memorandum has been coordinated with the City Manager's Office, DOT, PRNS, and City Attorney's Office.

CEQA

Not a Project, File No. PP17-009, Staff Reports, Assessments, Annual Reports, and Informational Memos that involve no approvals of any City action.

/s/
ANTHONY MATA
Chief of Police

/s/
KHALED TAWFIK
Chief Information Officer

For questions, please contact Albert Gehami, City Digital Privacy Officer, at (408) 793-6878 or digitalprivacy@sanjoseca.gov.

Attachments

Data Usage Protocol for Automated License Plate Reader Technology

City of San José

Data Usage Protocol (DUP) for Automated License Plate Reader (ALPR) Technology

Owning department(s): San José Police Department (SJPD)
Department owner: Deputy Chief, Executive Officer

1) Purpose

Automated License Plate Readers (ALPRs) use high speed cameras to photograph vehicle license plates. The purpose of ALPR cameras is to improve criminal investigations[1] and deter crime in the surrounding area.[2] 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 ALPR technology that complies with State and local laws;
2. Annual reporting requirements on ALPR usage; and
3. An ongoing avenue for public feedback on ALPR usage.

This DUP is also meant to ensure that San Jose Police Department's use of Automated License Plate Recognition (ALPR) technology complies with all applicable federal, state, and local laws. For the purposes of California law, this document serves as the "usage and privacy policy" as required by California Civil Code Sections 1798.29 and 1798.82.

2) Authorized Uses:

The Department shall use ALPR technology with the goal of reducing serious crime and traffic incidents in the long term. ALPR is meant to act as a deterrent for crime and dangerous driving in a neighborhood, and to support police in criminal investigations. ALPR vendors may only use the data if authorized by the City to act on behalf of the City. The Department and authorized vendors may utilize ALPR technology and any data generated only to do the following:

1. Use in conjunction with any patrol or investigative function in response to the investigation of felony or misdemeanor crimes;
2. Locate at-risk missing persons (including responding to Amber and Silver Alerts);

[1] Koper, Christopher S., and Cynthia Lum. "The impacts of large-scale license plate reader deployment on criminal investigations." *Police Quarterly* 22.3 (2019): 305-329 – https://journals.sagepub.com/doi/abs/10.1177/1098611119828039

[2] Koper, Christopher S., Bruce G. Taylor, and Daniel J. Woods. "A randomized test of initial and residual deterrence from directed patrols and use of license plate readers at crime hot spots." *Journal of Experimental Criminology* 9.2 (2013): 213-244 – https://link.springer.com/article/10.1007/s11292-012-9170-z

3. Support local and State safety departments in the identification of vehicles associated with criminal investigations. Further detail on permissible sharing and coordination with safety departments is detailed in the "Data Sharing" section below; and
4. Automatically initiate investigation for traffic intersection infractions through a device (e.g., red-light violations) if SJPD follows the requirements outlined in California Vehicle Code 21455.5,[3] including providing notice of automated enforcement within 200 feet of the intersection.

3) Prohibited Uses:

ALPR technology will not be used for the following purposes:

1. Collect data that is not within the public view. This includes any data not readily visible from a public area or public property;
2. Monitor individual or group activities legally allowed in the State of California and/or protected by the First Amendment to the United States Constitution;
3. Share with immigration authorities or use in the investigation of any matter related to immigration status of an individual;
4. Engage in automated citations or other automated enforcement without manual review from SJPD staff; and
5. Sell any data generated by ALPR to any entity.

4) Operational Procedures

The ALPR system(s) and their associated database(s) shall only be used for official law enforcement purposes listed in the "Authorized Uses" section. Additionally:

1. No member of the Department shall operate, utilize and/or search ALPR systems and their associated equipment/database(s) without first completing Department-approved training and only if the operation, utilization, or searching complies with SJPD's need to know/right to know protocols defined in SJPD Duty Manual section C2000 on criminal records and information;[4]
2. Once an alert is received, the officer will make every effort to visually confirm that the captured license plate from the ALPR system matches the license plate of the observed vehicle;
3. In all instances, before any action is taken based solely upon an ALPR alert, the officer will make every effort to verify the alert is still valid through the California Law Enforcement Telecommunications System (CLETS). Officers will not take any action that restricts the freedom of any individual based solely upon an ALPR alert until an attempt at verification has been made;
4. If the reason for an ALPR alert pertains to a wanted person associated with a vehicle, officers should attempt to visually inspect the occupant(s) of the vehicle to determine if he/she matches the description of the wanted individual. Absent this verification, officers must have a separate legal justification to conduct a vehicle stop;

[3] California Vehicle Code "Offenses Relating to Traffic Devices" - https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=21455.5.&nodeTreePath=15.2.3&lawCode=VEH

[4] See SJPD Duty Manual - http://www.sjpd.org/records/dutymanual.asp

5. Designation of vehicles into "hot lists"[5] shall be the sole responsibility of the assigned investigating officer or his/her designee. Vehicle's cannot be entered into "hot lists" without a lieutenant's approval. It will be the arresting/investigating officer's responsibility to ensure timely entry/removal of license plates into/out of the designated "hot lists".
6. To the best of the system administrator or his/her designee's ability, hot lists managed by an external source (e.g., the Stolen Vehicle System) will be synchronized with the external hot list at all times. In the event of a loss of connection to external hot lists, the ALPR system administrator or his/her designee shall synchronize with external hot-lists upon reconnection;
7. Protocols shall be established to ensure timely notification is made to the system administrator to indicate and record when a "hot list" ALPR license plate capture is made and the ultimate disposition of the specific enforcement action;[6] and
8. All vehicles entered into a departmental "hot list" will contain the following information:
    a. Name, badge number and assignment of department member entering the information (e.g., Officer Smith #1234, Robbery Unit)
    b. Associated case number(s)
    c. Short synopsis describing the reason for the vehicle/occupant database entry. This should include the presumed crime or crimes relevant to this investigation. If no crime is relevant, state the other purpose (e.g., Amber alert)

5) Data Collection

ALPR utilizes high speed cameras angled to capture digital images of vehicle license plates on public roads and private property visible from a public road (e.g., a driveway). The cameras are trained on the license plate of a vehicle and rarely capture the image of a person. The cameras do not identify an individual or group based on physical characteristics such as skin-tone, body shape, or facial features.

An example image captured from an ALPR camera is provided in Figure 1. While the ALPR camera is angled to capture license plate information, it may collect additional information visible in the image, including car make/model, and other distinguishing characteristics of the vehicle (e.g., bumper sticker(s), after market wheels, etc.).

ALPR cameras may be placed in a fixed location, such as on a street light pole, or in a roaming location, such as on a police vehicle. The technology will record the date and time the image was captured as well as the location of the camera. The exact location of a vehicle is not tracked, but can be inferred based on the location of the camera at the time of the photograph.

[5] License plate(s) associated with vehicles of interest from an associated database, including, but not limited to: California Law Enforcement Telecommunications System (CLETS), National Crime Information Center (NCIC), Be on the Lookout notices (BOLOs), and Department databases

[6] An example notification would be: "Hot list 211A vehicle alerted at Curtner/Monterey, observed at Curtner/Malone. Vehicle stopped, driver arrested for 211"

Figure 1: Police vehicle with an Automated License Plate Reader mounted on its roof, and an example picture from the ALPR camera (top-left). This ALPR picture identifies 1) the license plate, 2) the time and location of the car, and 3) other information captured in the photograph, including vehicle color, make, and model. Source: Pasadena, CA Police Department. https://www.pasadenanow.com/main/city-council-to-consider-purchasing-more-automatic-license-plate-readers

6) Notice

Notice that the City of San José is using ALPR technology will be posted as signage at major vehicle entrances into the city and exits from the city, and at "designated intersections" within the city to notify residents that ALPR cameras may be present in their area.

"Designated intersections" refers to locations near where ALPR technology is being utilized. The signs will contain notice that ALPR technology is in use and will direct the reader to where they can get more information about the ALPR program and policies. Notice and additional detail, including this Data Usage Protocol, will be available on the City website.

7) Retention and Minimization

Data collected from ALPR technology will be retained for one year. Once the retention period has expired, the record shall be purged entirely from all active and backup systems unless the data is related to an active investigation of a crime not listed in the "Prohibited Uses" section.

Data associated with a criminal investigation may be stored for longer on an electronic storage device or printed and retained 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.

8) Access and Accuracy

Raw ALPR data, including photographs, license plates, location, and associated hot list data will not be available for public access unless required pursuant to city, state, or federal law, or a court order. Aggregated data on the ALPR technology, including performance metrics on the accuracy of the technology, 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.

9) Accountability

All Department members authorized to use or access ALPR technology or data shall be accountable for knowledge of this protocol. See "Training" section for definition of authorized personnel.

All access to the system shall be logged, and the Department will maintain an audit trail of requested and accessed information, including the purpose of the query. Periodic, random audits shall be conducted by a unit other than Crime Data Intelligence Center (CDIC) at the direction of the Deputy Chief, Executive Officer 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 a minimum of two (2) years. Additional audits or reviews may be triggered at the direction of the City Council or Digital Privacy Officer (DPO), consistent with state law and authorized access to information.

If a Department member accesses or provides access to ALPR information, the Department member shall do the following:

1. Maintain a record of the access that includes the following information:
    a. Date/Time the Information was accessed
    b. The license plate number or other data elements used to query the ALPR system
    c. The name and department of the person who accessed the information
    d. The purpose for accessing the information, including the presumed crime or crimes relevant to this investigation. If no crime is relevant, state the other purpose (e.g., Amber alert)
2. ALPR information may only be used for authorized purposes as specified in this protocol in accordance with California Civil Code section 1798.90.51(b).

10) Sharing

The City does not share ALPR data with any contracted, commercial, or private entity. The provision of data hosting or towing services shall not be considered the sale, sharing, or transferring of ALPR information (see CA Civil Code 1798.90.55.(b)).

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 without authorization; 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 ALPR database by law enforcement agencies within the State of California on an agency-by-agency basis if an agreement is put into place.
The data will not be shared beyond the approved agencies. All agencies must request SJPD ALPR data directly from SJPD (e.g., if SJPD shares ALPR 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.

Logs will be generated every time an approved law enforcement agency accesses data from SJPD's ALPR system, which will include:

a. Date/Time the Information was accessed
b. The license plate number or other data elements used to query the ALPR system
c. The name and law enforcement agency of the person who accessed the information
d. The purpose for accessing the information

11) Equity and Community Engagement

The City will make a reasonable effort to identify and mitigate any inequity inherent in the ALPR technology 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. ALPR 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.

12) Storage and Security

Data collected by ALPR technology shall be stored in a secured police facility or secured third-party hosting environment. With the exception of audits, access to the raw data (images of vehicles and license plates) 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 ALPR data. Authorized sworn personnel or authorized civilian personnel (such as a crime analyst) shall have general user access to the SJPD ALPR database, as appropriate, to query information. See "Training" section for definition of "authorized personnel". Entities authorized to audit the ALPR system (see "Accountability" section for who can authorize) do not need to be a part of the Department to access the database.

Sworn personnel or authorized civilian personnel as approved by the Deputy Chief, Executive Officer, or his/her designee shall have administrative user access to the SJPD ALPR database, as appropriate, to control:

1. The information to which a particular group or class of users can have access based on the group or class;
2. The information a class of users can access, and/or data being utilized in specific investigations;
3. Sharing capabilities with other law enforcement agencies; and
4. Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the data or equipment.

The Bureau of Technical Services Systems Development Unit may provide ALPR technical support for the Criminal Data Intelligence Center (CDIC). The CDIC shall ensure compliance with this protocol. The custodian of ALPR data for purposes of this protocol shall be the Deputy Chief, Executive Officer or his/her designee.

In the event of a confirmed data breach where personal information such as license plate numbers or photographs have been accessed by an unauthorized party, the Department will follow the City of San José's Incident Response Plan. This security protocol and further security details are overseen by the City's Cybersecurity Office.

13) Training

Except for audits, only authorized personnel, meaning Department personnel trained in the use of ALPR technology, including its privacy and civil liberties protections, shall be allowed access to ALPR data. Training shall consist of:

1. Legal authorities related to the use of ALPR data and technology;
2. Current Department Data Usage Protocol regarding authorized use of ALPR technology;
3. Technical, physical, administrative, and procedural measures to protect the security of ALPR data against unauthorized access or use; and
4. Practical exercises in the use of ALPR technology.

14) Annual Data Usage Report requirements

To provide the City and the public with ongoing reporting on the usage and accuracy of the ALPR technology, 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.[7] 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

[7] 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

the DPO needs additional time, they shall provide a notice of extension to the public via the Digital Privacy webpage.[8]

1. Summary of the project and updates since the prior year, including detail on value to the department
2. Plans for future years, including any planned expansion of project or shift in data usage
3. Reporting metrics on ALPR usage and accuracy including:
    a. **# of reads by location** – the Department will either:
        i. Report directly the number of reads by location; or
        ii. Provide the Digital Privacy Officer (DPO) with access to the ALPR reads database, including the latitude and longitude of each read, from which the DPO can report by location as needed.
    b. **# of hits by location** – Similar to the # of reads by location, the Department will either:
        i. Report directly the number of hits by location; or
        ii. Provide the DPO with access to the ALPR reads database, including the latitude and longitude of each read and if the read was a hit, from which the DPO can report by location as needed.
    c. **Records accessed by SJPD** – the Department will report on the number of records accessed in accordance with the Accountability section of this Protocol.
    d. **Accuracy of accessed records** – the Department will report on the accuracy of the implemented ALPR technology as requested by Council and the DPO

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