

Public comments - agenda item 3.5 of the San José City Council meeting on September 20, 2022

Chi-Kai Sin <[REDACTED]>

Mon 9/19/2022 11:10 AM

To: Chi-Kai Sin <[REDACTED]>; City Clerk <city.clerk@sanjoseca.gov>; The Office of Mayor Sam Liccardo <TheOfficeofMayorSamLiccardo@sanjoseca.gov>; District1 <district1@sanjoseca.gov>; District2 <District2@sanjoseca.gov>; District3 <district3@sanjoseca.gov>; District4 <District4@sanjoseca.gov>; District5 <District5@sanjoseca.gov>; District 6 <district6@sanjoseca.gov>; District7 <District7@sanjoseca.gov>; District8 <district8@sanjoseca.gov>; District9 <district9@sanjoseca.gov>; District 10 <District10@sanjoseca.gov>

 1 attachments (223 KB)

public comments - item 3.5 of San Jose City Council meeting 09-20-2022.pdf;

[External Email]

You don't often get email from [REDACTED]. [Learn why this is important](#)

[External Email]

Dear Mayor, Councilmembers, and City Clerk,
On behalf of several community organizations, I am submitting the attached letter (pdf file) as written public comments for agenda item 3.5, "Digital Privacy Program Update and Public Camera Use," of the San José City Council meeting on September 20, 2022.
Thank you for your kind attention.
Respectfully,
Victor Sin
Chair (volunteer), Santa Clara Valley Chapter of the ACLU of Northern California

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

This message is from outside the City email system. Do not open links or attachments from untrusted sources.



Coalition for Justice and Accountability
"Building a community where everyone feels safe."

September 19, 2022

200 E. Santa Clara Street,
San José CA 95113

Re: Agenda item 3.5, "Digital Privacy Program Update and Public Camera Use," of the San José City Council meeting on September 20, 2022

Dear Mayor and Councilmembers,

The undersigned organizations are community organizations in the San José area that are dedicated to protecting civil rights and civil liberties, including the right to be free from intrusive, discriminatory, and dangerous government surveillance. We continue to express strong opposition to the proposed deployment of Automatic License Plate Systems (ALPRs) in San José.

As explained in details in the written public comments submitted by the Santa Clara Valley Chapter of ACLU of Northern California to the PSFSS Committee (<https://sanjose.legistar.com/View.ashx?M=F&ID=10661349&GUID=2EE5541A-3A8E-445B-8937-C0EC33879172>), ALPR systems will make our community less, not more, safe. Despite claims that ALPR systems can reduce crime, researchers have expressed concerns about the rapid acquisition of this technology by law enforcement without evidence of its efficacy. Multiple studies have found no relationship between the deployment of ALPR and vehicle thefts. Instead, ALPR systems have been shown to violate privacy, facilitate dangerous police stops¹, and risk exposing our immigrant community members to harm.

Recognizing that the City Council already approved the ALPR project at the Monterey-Curtner intersection on September 21, 2021 and approved the allocation of \$250,000 for another ALPR project on November 30, 2021, we strongly urge the City Council to mitigate the impact on civil liberties and privacy by adopting a strong, comprehensive, and thorough Data Usage Protocol ("DUP"). We appreciate the City's effort to incorporate some of ACLU's feedback to the Digital

¹ See <https://www.aclu.org/news/privacy-technology/san-francisco-woman-pulled-out-car-gunpoint-because>

Privacy Advisory Taskforce to protect our privacy, but we still have a number of outstanding concerns that the DUP does not go far enough to ensure our civil liberties are being protected.

Section 2 of the DUP states, “The Department and authorized vendors may utilize ALPR technology and any data generated only to do the following: ...” The policy should specify the scenarios in which third-party vendors should be allowed to access the data, much less *use* the data. We question why third-party vendors would need to use the data, and are concerned about personal data being accessed and used by more people and institutions. The policy should specify what types of third-party vendors are included, and the specific situations in which access is necessary.

Usage of ALPR systems for low-level, nonviolent incidents like traffic infractions, as listed in item 4 of Section 2, only opens more community members to further-reaching government surveillance. We caution the city to consider how using these systems for low-level issues can have unintended and disproportionate impacts on communities who already experience over-policing, such as Black people, immigrants, and Muslim communities.

SB 34, codified as Civil Code, Division 3, Title 1.81.23, prohibits a public agency from sharing, transferring, or making available ALPR information, defined in the law to include “information or data collected through the use of an ALPR system,” to entities that are not California public agencies, such as federal or out-of-state government agencies. The Policy should reflect this law and its sharing restriction. While we recognize that the DUP does not mention sharing data with out-of-state agencies, explicit language prohibiting sharing with federal or out-of-state government agencies should be included to fully comply with SB 34.

As we shared in previous feedback to the Digital Privacy Advisory Task Force, usage of ALPR systems should be prohibited in the investigation of low-level offenses such as minor drug offenses, prostitution, loitering, and graffiti.

We continue to urge the city to shorten the data retention period. Data retention for one year will amass an enormous trove of data. If there are specific incidents that are of concern to law enforcement, the policy can be written to allow data related to those incidents to be preserved for a longer period of time, instead of a blanket one-year retention period.

As part of accountability, the DUP should state that the audit logs will be available to any individual charged with a crime as a result of ALPR usage.

We have concerns about the proposed sharing policy, described in Section 10 of the DUP, which would allow the city to “...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.” We strongly urge the city to limit the sharing of ALPR data. Moreover, the policy should prohibit the sharing of ALPR data with California agencies unless they agree to prohibit further sharing with out-of-state and federal agencies. Finally, law enforcement should be prohibited from sharing ALPR data with any law enforcement agency for purposes of enforcing prohibitions on reproductive or gender-affirming care, or interstate travel for reproductive or gender-affirming care.

Moving forward, we urge the City to engage community members in a discussion about non-surveillance alternatives to ALPR that have been demonstrated to actually improve the health and safety of communities like our own. The Digital Privacy Advisory Task Force was consulted only after the Monterey-Curtner APLR project was approved by City Council. Similarly, city staff was asked to work out privacy concerns after approval. This process operates under the assumption that surveillance technologies will always outweigh the cost to civil liberties and that privacy can be protected and harms mitigated. This is simply not true. These technologies pose significant risks and deserve the time and attention of thorough consideration and community involvement. Pursuant to the backlogged list of 2021 priority setting, we encourage the relevant Committee and City Council to pursue adoption of a Surveillance Technology Ordinance to codify best practices for meaningful community engagement and to ensure transparency, accountability, and oversight for all proposals to acquire or use surveillance technology.

Thank you very much for your kind attention.

Sincerely,

Victor Sin
Chair (volunteer)
Santa Clara Valley Chapter of ACLU of Northern California

Richard Konda
Executive Director
Asian Law Alliance

Aram James
Director of Advocacy
Coalition for Justice and Accountability

Bob Nuñez
President
San Jose / Silicon Valley NAACP

Ruth Silver Taube
Coordinator
Santa Clara County Wage Theft Coalition

Public Comment 9/20/2022 Meeting - Agenda Item 3.5 22-1387

Masheika Allgood <[REDACTED]>

Mon 9/19/2022 3:39 PM

To: City Clerk <city.clerk@sanjoseca.gov>

[External Email]

You don't often get email from [REDACTED]. [Learn why this is important](#)

[External Email]

Hello Mayor, Councilmembers, and City Clerk,

I am submitting the attached memo (pdf file), on behalf of the Black Leadership Kitchen Cabinet, as written public comments for agenda item 3.5, "Digital Privacy Program Update and Public Camera Use," of the San José City Council meeting to be held on September 20, 2022.

Masheika Allgood
Chair BLKC Technology Advocacy Committee

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

This message is from outside the City email system. Do not open links or attachments from untrusted sources.



9/19/2022

San Jose City Councilmembers,

The SJ city council is being asked to approve a new ALPR DUP in advance of the placement of 150 video cameras at intersections all over the city. To anchor this memo, we'll begin with a discussion of what an ALPR system is. The video cameras that you are being asked to approve will capture video of all of the traffic at those intersections - every car that passes by, every child who goes through the crosswalk, the comings and goings at the homes and businesses in the immediate vicinity, everything. The cameras themselves aren't special technology, they're just video cameras. They capture video of everything in their range.

The videos that the cameras collect will be sent back to a data center for storage and processing. The 3rd party vendor owns the data pipeline that sends data from the cameras to the storage facility. The 3rd party vendor also owns and/or controls the storage facility. Once the raw footage is in the data warehouse, the 3rd party vendor runs it through software that is trained to identify license plates. So, to be clear, there is no such thing as an automated license plate reader. There is a system of video cameras that collect footage just like any other video camera. ALPR refers to the data processing step that happens after the footage is collected and stored, when it's run through a system that pulls out the license plate images in an automated way.

[SJPD signed a contract with Flock](#) for the pilot phase of this project. In that contract it states that Flock has no right to own or process any of the raw data that is being collected by the cameras. It also requires Flock to perform the process of de-anonymizing the raw data. De-anonymizing is the process of removing any data that could be used to identify a particular person. So, Flock must collect and store the raw data, and go through it to remove identifying characteristics, but they must never process the raw data. Clearly these mandates are mutually exclusive. So which responsibility are they contractually obligated to perform?

And what does it mean to de-identify the data? Do they have to remove the faces in the cars? What about the faces of the people walking in the street or entering houses or businesses? What about other identifying characteristics like a hair style, or a dog, or a bumper sticker? What if the frequency of timing of visiting a business makes someone identifiable? Do people need to be completely removed from the footage for this effort to be successful? And what happens to the raw data after the De-anonymized version is created? Is it destroyed? Is it stored as a backup?

While the rulemaking for the SJPD's use of ALPR data is controlled by a use of force policy, the requirements for Flock and their employees is controlled by the contract between Flock and the SJPD. Which means questions about Flock's responsibilities under that contract are legal questions. The issues discussed above are only a few of the myriad open questions that are raised by this partnership with Flock. None of which are clearly addressed in the initial contract. Specifically:

Procedural concerns:

- What is the contract term (it's apparently controlled by a separate document)?
- What constitutes a breach by Flock (the Terms & Conditions only discuss hardware delivery)?
- What happens if Flock gets hacked? Is there an addendum covering cybersecurity or ransomware?
- What if a Flock employee provides video from the cameras around medical facilities to government officials in states where abortions are banned? Are there any contractual provisions for internal controls?
- What happens if the Flock software is only 70% accurate? Or 50%? Does the City have any right to suspend the contract? What are the key performance indicators for the initiative? What is the service-level agreement (SLA)? Are there any requirements for Flock's software?
- What kind of notice does Flock have to give for platform and/or algorithm changes?

Definitions:

- The contract clearly defines hardware components. But the actual license plate reading function is not hardware based, it's software. How are software components defined?
- The contract discusses which party owns the hardware. Is storage considered hardware, software, or both?
- How are 'anonymized' and 'de-identified' defined?
- Does the definition of 'defect' cover incorrect results (misidentified vehicles)?

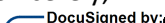
Logistical questions:

- Which party bears responsibility for ensuring that the raw data is fully de-identified/anonymized?
- In the event that the raw data isn't fully de-identified/anonymized and that causes injury to a citizen, who would the citizen sue?
- Where is the raw data stored? Who owns the storage?
- Which party is responsible for the security and integrity of the raw data before it is de-identified/anonymized?
- What is the process for citizens to correct misidentified vehicles?

The ALPR system will directly provide data to two entities - the SJPD and Flock. To date, all of the rulemaking and public outreach efforts around this partnership have been focused on just one of these entities - SJPD. But the city council's mandate requires the body to ensure that both entities respect citizen rights and act in the city's best interest. The recently updated DUP is a document regulating how the SJPD and DOT will use the ALPR data. However, Flock is not required to abide by any of the rules or regulations in the DUP. Flock is only legally obligated to abide by the requirements listed in the contract with the SJPD.

There are significant concerns with the contract that the SJPD has signed with Flock. We ask that the city council defer any vote on approving the ALPR-focused material in the DUP or expanding the ALPR program until a full and transparent legal analysis of Flock's legal responsibilities under the contract has been performed by the Office of the City Attorney.

Sincerely,

DocuSigned by:


Jahmal Williams
Co-Chair