City of Seattle

2023 Surveillance Impact Report

AUTOMATED LICENSE PLATE RECOGNITION (ALPR) (FLEET-WIDE)

Seattle Police Department

City of Seattle

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle IT Policy PR-02, the "Surveillance Policy".

How this Document is Completed

This document is completed by the requesting department staff, supported and coordinated by the Seattle Information Technology Department ("Seattle IT"). As Seattle IT and department staff complete the document, they should keep the following in mind.

1. Responses to questions should be in the text or checkboxes only; all other information (questions, descriptions, etc.) Should **not** be edited by the department staff completing this document.
2. All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

City of Seattle

Privacy Impact Assessment

Purpose

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. A PIA asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a Privacy Impact Assessment Required?

A PIA may be required in two circumstances.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

Seattle Police Department facilitates the flow of traffic (by monitoring and enforcing City parking restrictions) and recovers lost and stolen property through a number of means including Automated License Plate Reader (ALPR) technology. ALPR is utilized in the recovery of stolen vehicles, to assist with active investigations, Scofflaw Law enforcement, and parking enforcement.

This Surveillance Impact Report focuses on SPD use of ALPR as a necessary law enforcement tool in two capacities:

1. Property Recovery – SPD employs ALPR to locate stolen vehicles, as well as vehicles associated with a court-issued warrant.
2. Investigation – On occasion, SPD relies on license plate data to locate vehicle placement within the past 90 days (retention period), in the course of an active investigation or in support of legal proceedings.

Note that ALPR usage for parking enforcement is discussed in the Surveillance Impact Report entitled "Parking Enforcement Systems."

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

ALPR collects license plate information from vehicles, which could, if unregulated and indiscriminately used, be linked to other data to personally identify individuals.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed.

2.1 Describe the benefits of the project/technology.

ALPR assists the City in managing the flow of traffic by monitoring and enforcing City parking restrictions and locating and recovering lost/stolen property. Additionally, the ALPR system aids with active criminal investigations by helping to determine the location of vehicles of interest related to a specific case.

2.2 Provide any data or research demonstrating anticipated benefits.

General news reporting about ALPR Benefits: https://patch.com/california/glendora/plate-reader-helps-police-find-stolen-cars-make-warrant-arrests

2.3 Describe the technology involved.

Fleet-wide ALPR for SPD Patrol operations is a component of the Axon Fleet 3 in-car video platform.

The high-speed cameras capture images of license plates as they move into view, and associated software deciphers the characters on the plate, using optical character recognition. This interpretation is then immediately checked against any license plate numbers that have been uploaded into the onboard, in-vehicle software system. Twice a day, the License Plate Reader File (known as the HotList), a list of license plate numbers from the Washington Crime Information Center (WACIC) and the FBI's National Crime Information Center (NCIC), is uploaded into the ALPR system (via a connection to WACIC), which is a source of "hits" for the license plate reader system. The license plate numbers compiled on the HotList "may be stolen vehicles, vehicles wanted in conjunction with felonies, wanted persons, and vehicles subject to seizure based on federal court orders" (WSP Memorandum of Understanding No. C141174GSC; March 11, 2014). Other sources include the City of Seattle Municipal Court's scofflaw list and content uploaded for overtime and metered parking enforcement (which are covered in the Parking Enforcement Systems SIR). No ALPR data collected by SPD are automatically uploaded into any system outside of SPD.

SPD contracts with Axon to provide both ALPR enabled in-car video hardware and software for the Fleet 3 Hub software system through which camera reads are interpreted and administrative control is managed. This includes the ability to set and verify retention periods, track and log user activity, view camera "read" and "hit" data, and manage user permissions.

The configuration is designed such that the cameras capture the images and filter the reads through the linked Fleet 3 Hub software to determine if/when a hit occurs.

When the software identifies a hit, it issues an audible alert, and a visual notification informs the user which list the hit comes from – HotList; Scofflaw; time-restricted overtime parking.

A "HIT" triggers a chain of responses from the user that includes visual confirmation that the computer interpretation of the camera image is accurate, and the officer verbally checks with Dispatch for confirmation that the license plate is truly of interest before any action is taken. This is done to ensure the system is accurately reading license plates. When an inaccuracy is detected, users may choose to enter a note into the system that the "hit" was a misread.

All data collected by the ALPR systems – images, computer-interpreted license plate numbers, date, time, and GPS location – are stored and retained for 90 days. After 90 days, all data collected by the ALPR systems is automatically deleted (unless it has been flagged as serving an investigative purpose – in which case, it is included in an investigation file).

2.4 Describe how the project or use of technology relates to the department's mission.

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services. SPD's department priorities include the use of best practices that include officer safety guidelines and performance-based accountability to provide progressive and responsive police services to crime victims, witnesses, and all members of the community, and to structure the organization to support the SPD mission and field a well-trained sworn and non-sworn workforce that uses technology, training, equipment, and research strategically and effectively.

Seattle Police Department uses ALPR technology in its pursuit of maintaining public safety and enforcing applicable laws related to stolen vehicles and other crimes.

2.5 Who will be involved with the deployment and use of the project / technology?

All SPD vehicles with onboard in-car video will have ALPR functionality enabled. All sworn SPD officers will be trained in the use of the in-car video with ALPR enabled functionality.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City are bound by restrictions specified in the surveillance ordinance and privacy principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

The ALPR system is used passively to receive reads and hits, actively to coordinate resources during an active event, or for investigative purposes based on historical reads. All officers equipped with an ALPR system will be trained prior to gaining any access to the ALPR system. Once this training has been verified with the ALPR administrator, users are given access and must log into the system with unique login and password information whenever they employ the technology. They remained logged into the system the entire time that the ALPR system is in operation. The login and use history is logged and can be audited. Patrol Officers are assigned the vehicles to use while on-shift. Access to the historical reads is limited to specific authorized individuals permanently assigned to the Real Time Crime Center and/or Intelligence Units and who have completed training on the ALPR system. If individuals are transferred out of those units, their permissions to the system will be revoked. Any request to search the historical reads by any officer must be accompanied by a written request identifying the requestor, the reason for the search, including the reasonable suspicion or probable cause and the associated case number, and submitted to an authorized individual to perform the search. As with all access to the ALPR system, every access and search is logged in the system. Access and use of the system will be audited by the SPD Audit Unit and the Office of the Inspector General.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

ALPR systems can be used during routine patrol, specific to a criminal investigation (i.e., to locate a stolen vehicle), or parking enforcement as per SPD Policy 16.170. The policy requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. In addition, the policy limits use of the technology to strictly routine patrol or criminal investigation. Further, the policy clarifies that users may only request access to historical ALPR data when that data relates to a specific criminal investigation as described above. A record of these requests is maintained by the ALPR administrator and subject to auditing by SPD Audit Unit and the Office of the Inspector General.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

SPD Policy 16.170 addresses Automatic License Plate Readers. The policy requires that users must be trained; they must be certified in A Central Computerized Enforcement Service System (ACCESS) – a computer controlled communications system maintained by Washington State Patrol that extracts data from multiple repositories, including Washington Crime Information Center, Washington State Identification System, the National Crime Information Center, the Department of Licensing, the Department of Corrections Offender File, the International Justice and Public Safety Network, and PARKS - and trained in the proper use of ALPR. Further, the policy clarifies that users may only request access to historical ALPR data when that data relates to a specific criminal investigation as described above. A record of these requests is maintained by the ALPR administrator and subject to auditing by SPD Audit Unit and the Office of the Inspector General.

4.0 Data Collection and Use

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other City departments.

Data collected from ALPR includes license plate image, computer-interpreted read of the license plate number, date, time, and GPS location.

All ALPR-equipped vehicles upload a daily HotList that contains only license plate numbers, with the associated states, that are under active search warrant from NCIC and WASIC.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

When the ALPR system registers a hit – a match to license plate number listed on the HotList (as described in 2.3 above) - the user must verify accuracy before taking any action. For instance, when the system registers a hit on a stolen vehicle, the user must visually verify that the system accurately read the license plate and, if so, must then contact Dispatch to verify accuracy of the hit – that the vehicle is actually listed as stolen. Only then does the user take action.

Unless a hit has been flagged for investigation and exported from the database for this purpose, all captured data will be automatically deleted after 90 days, per department retention policy.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

In-car video systems with enabled ALPR will be used in Patrol on a daily basis by authorized police officers (see 2.5 above).

4.4 How often will the technology be in operation?

In-car video systems with enabled ALPR will be used in Patrol on a daily basis by authorized police officers (see 2.5 above).

4.5 What is the permanence of the installation? Is it installed permanently, or temporarily?

Fleet-wide ALPR is a component of permanently installed in-car video.

4.6 Is a physical object collecting data or images visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

Fleet-wide ALPR is a component of permanently installed in-car video. Most SPD vehicles which have in-car video units installed are clearly marked as police vehicles. In-car video with enabled ALPR is installed in a few unmarked SPD vehicles which also have in-car video units.

4.7 How will data that is collected be accessed and by whom?

Only authorized users can access the data collected by ALPR. Per SPD Policy 16.170, authorized users must access the data only for active investigations and all activity by users in the system is logged and can be audited. SPD personnel within specific investigative units have access to ALPR data during its retention window of 90 days, during which time they can reference the data if it relates to a specific investigation.

Data removed from the system/technology and entered into investigative files is securely inputted and used on SPD's password-protected network with access limited to detectives and identified supervisory personnel.

SPD employee access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

ALPR systems are operated and used only by SPD personnel.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Users can only access the equipment for purposes earlier outlined (see 1.0) – recovery of lost or stolen property, to assist with active investigations, Scofflaw Law enforcement, and parking enforcement. Per SPD Policy 16.170, "ALPR may be used during routine patrol or any criminal investigation," and users can access "patrol ALPR data only when the data relates to a specific criminal investigation."

4.10 What safeguards are in place for protecting data from unauthorized access (encryption, access control mechanisms, etc.) And to provide an audit trail (viewer logging, modification logging, etc.)?

Individuals can only access the ALPR system via unique login credentials. Hardware systems can only be accessed in-vehicle. As previously noted, all activity in the system is logged and can be audited.

SPD's Audit Unit can conduct an audit of the system at any time. The Office of Inspector General and the federal monitor can also access all data and audit for compliance at any time.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

All data collected from the ALPR system is stored, maintained, and managed in a CJIS certified evidence retention platform. Retention is automated, such that unless a record is identified as being related to a criminal investigation and exported in support of that investigation, all ALPR data is deleted after 90 days. No backup data is captured or retained.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

SPD's Audit Unit can conduct an audit of any SPD system at any time. In addition, the Office of Inspector General can access all data and audit for compliance at any time.

SPD conducts periodic reviews of audit logs and they are available for review at any time by the Seattle Intelligence Ordinance Auditor under the City of Seattle Intelligence Ordinance. The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

5.3 What measures will be used to destroy improperly collected data?

Once a license plate has been read, this data is automatically retained for a period of 90 days. Unless the data is needed for a specific investigation, it is automatically deleted after 90 days.

5.4 which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Seattle City IT, in conjunction with SPD's ALPR administrator, is responsible for ensuring compliance with data retention requirements. Additionally, external audits by OIG and the Federal Monitor can review and ensure compliance, at any time.

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

No person, outside of SPD, has direct access to the ALPR system or the data while it resides in the system.

Data obtained from the system may be shared outside SPD as required by law.

Data may be shared with outside entities in connection with criminal investigations and prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by the ALPR may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly executed research and confidentiality agreements as provided by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the ALPR system.

6.2 Why is data sharing necessary?

Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process.

Products developed using this information may be shared with other law enforcement agencies. All products created with the information used in this project will be classified as Law Enforcement Sensitive. Any bulletins will be marked with the following restrictions: LAW ENFORCEMENT SENSITIVE — DO NOT LEAVE PRINTED COPIES UNATTENDED — DISPOSE OF IN SHREDDER ONLY – NOT FOR PUBLIC DISPLAY OR DISTRIBUTION — DO NOT FORWARD OR COPY.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or manner in which the [system or technology] may be used.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

System users are trained to visually verify accuracy, comparing a license plate hit to the physical plate/vehicle that the system read before taking any action. If they note a misread, they can enter a note into the system recognizing the read, as such. If they cannot verify visually, no action is taken.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

ALPR use is not legally constrained at the local, state, or federal level. Instead, retention of data is restricted. SPD retains license plate data that is not case specific (i.e., related to an investigation) for 90 days.

Case specific data is maintained for the retention period applicable to the specific case type.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Each component of data collected, on its own, does not pose a privacy risk. Paired with other known or auditable information, however, an individual may be able to personally identify owners of vehicles, and then use that information to determine, to a certain degree, where specific vehicles have been located. Because SPD's fleet-wide ALPR cameras are not fixed in location and records are only retained for 90 days, privacy risk is substantially mitigated because of the limited ability to identify vehicle patterns.

Per SPD Policy 16.170, general users of ALPR are restricted from accessing the data, except as it relates to a specific criminal investigation. Any activity by a user to access this information is logged and auditable. The PRA requires release of collected ALPR data, however, making it possible for members of the general public to make those identification connections on their own if they have access to the information necessary to do so, such as an independent knowledge of a particular individual's license plate number.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

As mentioned in 7.3, the data could be used to personally identify individuals; however, SPD policy prohibits the use of data collected by ALPR to be used in any capacity beyond its relation to a specific criminal investigation or parking enforcement action. Additionally, all collected data that is not relevant to an active investigation is automatically deleted after 90 days of collection.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Data collected by ALPR is only disclosed pursuant to the public under the PRA. The only data available for disclosure is that data which remains in the system within the 90-day retention window.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Any requests for disclosure are logged by SPD's Public Disclosure Unit. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

The ALPR system does not self-audit. Instead, third party audits exist, as follows: 1) The ALPR administrator has the responsibility of managing the user list and ensuring proper access to the system; 2) The Federal Monitor can conduct an audit at any time; and 3) the OIG can also conduct an audit. Violations of policy may result in referral to Office of Police Accountability (OPA).

SPD's Audit Unit personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
2024	2024	$0	-	-	

Notes:

The hardware needed for the fleet-wide ALPR system is part of SPD's in-car video system, so there are no acquisition costs associated with turning the ALPR portion on.

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☐ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source
$280,000	-	$77,000	TBD	General Fund

Notes:

The costs for fleet-wide ALPR software, hardware, maintenance, and support are annual and ongoing.

1.3 Cost savings potential through use of the technology

There are not expected to be any cost savings from this technology, only increased ability to locate stolen and wanted vehicles.

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
Washington State Patrol		

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use
Bryce Newell, PhD	Brycenewell@uky.edu	"Transparent Lives and the Surveillance State: Policing, New Visibility, and Information Policy" – A Dissertation

3.0 White Papers or Other Documents

Please list any authoritative publication, report or guide that is relevant to the use of this technology or this type of technology.

Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement	US Department of Justice (federally-funded grant report)	https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf

Racial Equity Toolkit ("RET") and engagement for public comment worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.
☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.
☐ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.
☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

Without appropriate policy, license plate data could be paired with other identifiable information about individuals that could be used to identify individuals without reasonable suspicion of having committed a crime, or to data mine for information that is not incidental to any active investigation. SPD Policy 16.170 mitigates this concern by limiting operation to solely routine patrol, criminal investigations, and parking enforcement.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

Trust in SPD is impacted by its treatment of all individuals. Equity in treatment, regardless of actual or perceived race, gender, sex, sexual orientation, country of origin, religion, ethnicity, age, and ability is critical to establishing and maintaining trust.

Per the 2016 Race and Social Justice Initiative Community Survey, measuring "the perspectives of those who live, work, and go to school in Seattle, including satisfaction with City services, neighborhood quality, housing affordability, feelings about the state of racial equity in the city, and the role of government in addressing racial inequities," 56.1% of African American/Black respondents, 47.3% of Multiracial respondents, and 47% of Indian/Alaska Native respondents have little to no confidence in the police to do a good job enforcing the law, as compared with 31.5% of White respondents. Further, while 54.9% of people of color have a great deal or fair amount of confidence in the police to treat people of color and White people equally, 45.1% of people of color have little to no confidence in the police to treat people equitably. This is contrasted with White respondents, of which 67.5% have a great deal or fair amount of confidence in the police to treat people of color and White people equally. This may be rooted in feelings of disparate types of contact with the police, across racial groups. While 14.3% of White respondents, 14.7% of Asian/Pacific Islander respondents, and 16.7% of Latino/Hispanic respondents reported being questioned by the police, charged, or arrested when they had not committed a crime, some communities of color reported much higher rates (American Indian/Alaska Native -52.7%; Black/African American - 46.8%; and Multiracial - 36.8%) of this type of contact with the criminal justice system.

As it relates to ALPR, it is important that SPD continue to follow its policy of limiting use of the technology to strictly routine patrol or criminal investigation, as well as limiting access to ALPR data to only instances in which it relates to a specific criminal investigation. Further, continuing to audit the system on a regular basis, provides a measure of accountability. In doing so, SPD can mitigate the appearance of disparate treatment of individuals based on factors other than true criminal activity.

1.4 Where in the City is the technology used or deployed?

☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle) (Mutual Aid)
- ☒ Outside King County (Mutual Aid)

If possible, please include any maps or visualizations of historical deployments / use.

If possible, please include any maps or visualizations of historical deployments / use here.

1.4.1 What are the racial demographics of those living in this area or impacted by these issues?

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

1.4.2 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

Per SPD Policy 16.170, "Before employees operate the ALPR system or access ALPR data, they will complete Department training on the proper and lawful use of the system." SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Also, by equipping all in-car video throughout the department with ALPR, deployment of this system becomes non-discretionary.

1.5 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Historically targeted communities have often been denied the same opportunities for information privacy as the majority populations. Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. In an effort to mitigate this possibility, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers. Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

1.6 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

As with decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities.

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

1.7 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

Without appropriate policy, license plate data could be paired with other identifiable information about individuals that could be used to identify individuals without reasonable suspicion of having committed a crime, or to data mine for information that is not incidental to any active investigation. SPD Policy 16.170 mitigates this concern by limiting operation to solely routine patrol, criminal investigations, and parking enforcement. 90-day data retention also mitigates the risk of improper identification of community members.

2.0 Public Outreach

2.1 Organizations who received a personal invitation to participate.

Public meetings are not required as part of the material change process; public comment was open from November to December 2023. General data can be found below and detailed public comment can be found in the appendix at the end of the document.

The initial public meeting information can be found in the original SIR (CB 120025).

3.0 Public Comment Analysis

This section will be completed after the public comment period has been completed on [DATE] by Privacy Office staff.

3.1 Summary of Response Volume

220 public comments were received during the public comment period. Below is the demographic data for public comment via Microsoft forms.

3.2 Question One: What concerns, if any, do you have about the use of this technology?

Please see appendix at end of document for detailed public comment.

3.3 Question Two: What value, if any, do you see in the use of this technology?

Please see appendix at end of document for detailed public comment.

3.4 Question Three: What would you want City leadership to consider when making a decision about the use of this technology?

Please see appendix at end of document for detailed public comment.

3.5 Question Four: General response to the technology.

Please see appendix at end of document for detailed public comment.

3.5 General Surveillance Comments

These are comments received that are not particular to any technology currently under review.

Please see appendix at end of document for detailed public comment.

4.0 Response to Public Comments

This section will be completed after the public comment period has been completed on [DATE].

4.1 How will you address the concerns that have been identified by the public?

What program, policy and partnership strategies will you implement? What strategies address immediate impacts? Long-term impacts? What strategies address root causes of inequity listed above? How will you partner with stakeholders for long-term positive change?

5.0 Equity Annual Reporting

5.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

"Provide to the executive and the City Council a privacy and civil liberties impact assessment for each SIR that must be included with any departmental request for surveillance technology acquisition or in-use approval. The impact assessment shall include a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities. The CTO shall share with the working group a copy of the SIR that shall also be posted during the period of public engagement. At the conclusion of the public engagement period, the CTO shall share the final proposed SIR with the working group at least six weeks prior to submittal of the SIR to Council for approval. The working group shall provide its impact assessment in writing to the executive and the City Council for inclusion in the SIR within six weeks of receiving the final proposed SIR. If the working group does not provide the impact assessment before such time, the working group must ask for a two-week extension of time to City Council in writing. If the working group fails to submit an impact statement within eight weeks of receiving the SIR, the department and City Council may proceed with ordinance approval without the impact statement."

Working Group Privacy and Civil Liberties Assessment

A new Working Group Privacy and Civil Liberties Assessment is not required as part of the Surveillance Impact Report material update process. Please refer to the Privacy and Civil Liberties Assessment in the original SIR (CB 120025).

Submitting Department Response

Description

Provide the high-level description of the technology, including whether software or hardware, who uses it and where/when.

Purpose

State the reasons for the use cases for this technology; how it helps meet the departmental mission; benefits to personnel and the public; under what ordinance or law it is used/mandated or required; risks to mission or public if this technology were not available.

Benefits to the Public

Provide technology benefit information, including those that affect departmental personnel, members of the public and the City in general.

Privacy and Civil Liberties Considerations

Provide an overview of the privacy and civil liberties concerns that have been raised over the use or potential mis-use of the technology; include real and perceived concerns.

Summary

Provide summary of reasons for technology use; benefits; and privacy considerations and how we are incorporating those concerns into our operational plans.

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

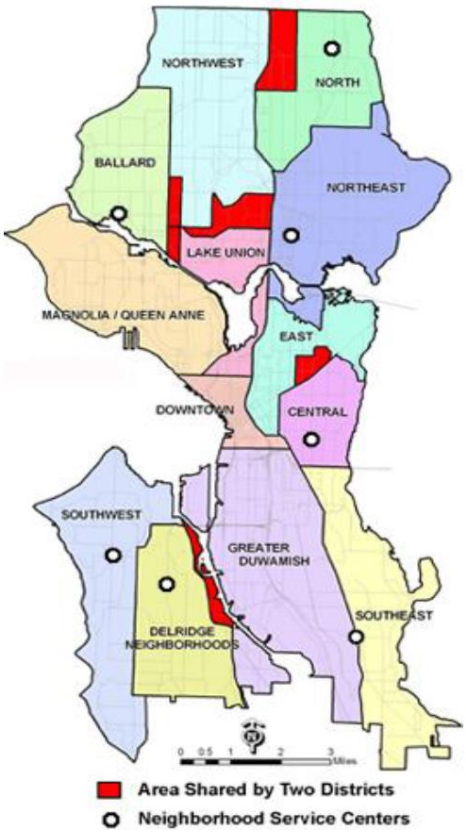
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

Appendix B: Public Comment Analysis

Responses to questions from the form:

1. What concerns, if any, do you have about the use of this technology?

ID	What concerns, if any, do you have about the use of this technology?
1	the 90-day searchable database of license plate reads is concerning. While using the ALPRs to find stolen property makes sense, the database of reads violates individuals' freedoms of movement and association. It also sounds like a potential violation of 4th amendment rights: SPD can scan someone's plate who is not involved in a crime and that information can be repeatedly searched over the course of 90 days.
2	The long retention of data
3	This is surveillance that increases risks for the public at large without providing a clear benefit to the public.
4	So many. Tracking of citizens who have not committed a crime would be unconstitutional. This data will be abused, cops are thugs and will do anything for power. Data hacking, info requests, and any myriad of other issues could come up. How many facists wanted to track everyone "just in case". Is 1% reduced crime worth my privacy, my views and my life? Nope
5	This is an insane surveillance overreach that has will cause more privacy violations than it will provide actual help in investigating actual crimes. Tracking and storing everyone's movements is so incredibly dystopian and I cannot believe this is even being considered. Just hire actual detectives and do real investigations.
6	Privacy, safety, accountability. The absurd claims that SPD can't delete these within two days, despite other forces doing it within minutes or hours. The ability of anyone to FOIA this information and use it to stalk, harass, or extort individuals. I also have serious concerns about trusting SPD with this technology, given the many documented cases over the past half decade of SPD officers inappropriately using this technology against specific civilians for personal reasons.
7	None
8	You will allow too many people to be able to track EVERYONE. For no reason. Having this data just sitting there is an intrusion into the everyones privacy.
9	The lengthy amount of time the data is kept on innocent people and the public availability of the data. The system should only be allowed to report hits on vehicles that are wanted for some reason. Saving the data on locations of all vehicles and making it available to FOIA requests could enable stalkers to track and harass victims. It would also let companies suck up huge amounts of data on the movements of people which could be repackaged and sold to anyone.
10	I am concerned about my privacy and the security of my personal data. I'm not comfortable with my location data being collected without my consent, and with that being stored for any length of time, nor with it being available to anyone who makes a public records request. I do not think I should have to give up this privacy in order to use Seattle streets.

11	License plate data is stored for far longer than reasonably necessary. License plates of vehicles not involved in any crime are identified and tracked. Benefits of this technology are statistically negligible and do not justify the invasion of privacy of all citizens.
12	Invasion of privacy, rights, and misuse of the technology to track people and vehicles.
13	I have many concerns. My chest is to complain about police using budget to purchase license plate scanning technology for all patrol cars. It is gross misuse of funds, budget, tax dollars.
14	This is a huge invasion of privacy, especially with its massive 90-day retention period of captured images of license plates. Stop this proposal altogether, or require SPD discard captured images immediately if not attached to an open case.
15	There is ample historical evidence that police in general, and SPD officers in particular, abuse databases for personal reasons and to target vulnerable populations such as undocumented immigrants.
16	Not only is it a concern that police can track individuals moves without any trace of criminal activity but the fact that an individual could do a public records request for your license plate is a danger for domestic violence victims.
17	I'm extremely concerned with the tracking of peoples vehicles even when their plates are unflagged. SPD should not be allowed to retain these unflagged plates for longer than it takes to scan the number
18	Enabling stalkers and abusive people to track their victims. The SPD needs to focus on crime rather than collecting even more info to analyze. That they keep the info for an inordinate amount of time shows they are not in a position to use the data for anything worthwhile. Taking away our ability to travel without being stalked is a major invasion of our rights. No evidence this reduces crime. Spend the money on prevention programs, not on unneeded, unproven and invasive technology.
19	Risks to privacy. Data companies submitting public information requests to obtain license plate and location data, then aggregating that data for sale. Even though the police only store the data for 90 days, anyone can request that data every 90 days and make them available either for free or for a fee. Imagine a website where you can enter your neighbors license plate and you can see where they have been at any time.
20	There are extremely limited use cases for this technology and I don't see the value for either the SPD or the public. This system will not prevent, detect or deter crimes and is solely a data collection service for a branch of civil government with a history of abusing access to this type of information. The cost could be better used in many other public services within the SPD, such as training and better screening of members of the police force for various abusive behaviors before they are members of the force. The numbers from the existing use cases do not justify an expansion of this program and if anything, justify the termination of this service and the redistribution of the funding. Tools that provide extensive surveillance information on random members of the public & gathered without cause need to be tightly controlled and regulated as there is little legitimate use for the system.

21	1. Documented history of abuse of official databases by police, explicitly including SPD. 2. Bad faith arguments supporting expansion. Why can other municipalities purge records in literally minutes but Seattle requires an indefinite period? 3. Value. Given the budget is perpetually thin, extraordinary evidence should be required before spending on dragnet surveillance efforts.
22	This is an incredibly terrible idea. What if someone makes a public records request for this information? If they knew your license plate number they could track you throughout the city, which would be an enormous invasion of privacy. I do not trust the city government to keep this information secure, and beyond that I see this as an expansion of police powers (via automation) that I am strongly against.
23	Abuse of power, stalkers will easily be able to find victims,
24	None
25	Having spent a significant amount of time in Europe, I don't have any concerns with the use of this technology.
26	Invasion of privacy.
27	It allows corruption to be legalized. Allowing so much power to law enforcement officers or citizens is asking for corruption. As much as 2% of vehicles in Seattle are on the hit list. The other 98% of vehicles should not be under scrutiny to tempt officers to track them, violating motorists privacy nor citizens. It would also deviate from time officers could be using to track criminal activity and apprehend suspects. It would also allow for more time with the officer's eyes on the APRL database instead of the road.
28	Being a victim of stalking. Having my location available for public record for a very long period of time.
29	Everything about it. This doesn’t belong in a freedom-oriented democracy. It feels like a surveillance state. It’s a matter of principle.
30	Retaining all images for 90 days is too long. And allowing anyone to access it is an absolute invasion of privacy. Only implement this after you have become able to determine whether a plate matches one of concern within 3 minutes. Then you can do it, but purge all other info every 3 minutes
31	None. ALPR technology is good tech for fighting crime.
32	Several SPD officers, still on staff, have been caught using police databases and technology to harass and stalk community members. This would be another technology that these officers could use for stalking and harassment.
33	Well if I had to choose one glaringly disturbing concern i could choose out of several, it would be our government making it even easier for violent and dangerous predators access to such a data rich archive consisting of any persons usual routes, places of business, children's school locations, and place of residence and all they would need is to have the victims license plate number. This should horrify any human with a 4th grade reading level.
34	Just put on brown shirts, it’ll be faster
35	It's unacceptable for SPD to retain license plate images for any durable period of time.
36	Police accessing records off duty.
37	I actually wanted to comment that this technology has helped local police to recover my '91 honda twice now and I am very much in favor of it.

38	That this information will be improperly used by individual malign actors in Seattle Police to target innocent people the officer has a bias against. The this information will be used systemically by the Seattle Police Department to establish a surveillance system that tracks people without reasonable suspicion or probable cause, and that this would result in a violation of people's fourth amendment right to privacy.
39	This is a constitutional issue. A citizen should continue to have the right and privilege of travelling freely without worrying about data collection or intrusion of this right. Unless a person is violating laws, then a citizen should be able to travel freely. Otherwise, this butts up again many violations of constitutional freedoms.
40	Concerns that this could be easily be abused, both by public inquiry (through public information request) and by the SPD itself.
41	I have many concerns, several around the potential for abuse of this system. - It sounds like any license plate can be stored and tracked, meaning abusive people will be able to track their targets through public records requests. There needs to be strict limits on deleting data timely. The 90 day limit is far too high. - Why are we allowing collection of license plate numbers that aren't connected to any crime? This should not be allowed. - I'm wary in general of increased surveillance. I'm not convinced this would even be helpful in solving crimes right now. - I think we need more privacy in general. This will mean one more entity tracking our every move. - Cops are fundraising to do genetic testing, and we want to spend public money on something like this. We know genetic testing works, so let's be thoughtful on how we spend our money! Spend it on something that works. (https://www.king5.com/article/news/crime/seattle-police-foundation-crowdfunding-dna-testing-cold-case/281-0a1c7cdb-1f9f-4395-91f9-fdc2068d5113) - I think this is too expensive. Cops are expensive already!! Can we make them more economical? I would prefer the city council spent more time addressing that question. - I live near a police station. I imagine I'm already getting tracked. It would be nice if we had safeguards on this, as I'm not a fan of being tracked. Please consider that instead of expanding the use of this technology!
42	Privacy. Personal intrusion.
43	As an information security engineer, privacy and data security. I do not trust anyone to store this data. I believe this is also a general invasion of privacy and I am strongly against mass surveillance. I do not even trust the city to properly control access to the data set and prevent abuse by city employees.
44	Automatically scanning license plates and making the data available for 90 days (or any length of time) is a significant breach of public safety and privacy. Once the data is available, there is no 90-day limit: parties interested in the data will scrape it regularly and keep it/sell it in perpetuity. The data will also be used by for personal, political, and other reasons to target and track public figures, individuals (like spouses, significant others, children) to stalk, harass, and commit crimes, such as abducting children subject to custody disputes.
45	Big brother
46	Surveillance is stalking. Stop it. Police already have too much power. We certainly don't need them stalking us. You know this will be used on communities of color, ex girlfriends or wives, in retaliation for complaints, etc. This is not a slippery slope but a landslide, destroying our freedom of movement. Next: see Hong Kong.
47	This is an unprecedented expansion of surveillance of the people in Seattle. It is warrant-less in both a legal and moral sense. It serves no purpose in line with its risks.
48	Gathering of surveillance data on people unconnected to crimes and police overstep.
49	Misuse, hacking.

50	The database this technology will compile (and the fact that SPD is allowed to hang on to this data for 90 days) can be easily exploited by police officers and the general public (via public records requests) to surveil anyone in Seattle, regardless of any law being broken or reasons to suspect a law will be broken. This seems like a violation of our civil right to privacy in our daily travel around the city.
51	It's unconstitutional 'big brother' surveillance.
52	Office of Police Accountability investigations have already shown that the SPD has abused this technology to track citizens for personal/non-crime related reasons
53	How long data on scans of license plates not on any hot list/non-hits are stored. 90 day retention policy is way too long, it creates a rolling 90 day map of where & when every car in Seattle was. This data can be requested by outside parties including law enforcement agencies in different states & private parties to create databases/maps showing where & when every car was in Seattle for much longer periods. Data on non-hits should not be retained beyond the few seconds it takes to check a license plate number against hot lists. There is no value in storing information on non-hits. And, there is no legitimate argument that it takes longer than a few seconds to check whether of not a license plate is on a hot-list.
54	I have no concerns, it will help reduce crime
55	Privacy. I do not need the Seattle Police tracking my movements and keeping that information in a publicly available database. Trust. The Seattle Police cannot be trusted with this information. As you might recall, they were placed under federal supervision because they are unable to uphold our constitutional rights. Accountability. The Seattle Police oppose accountability.
56	This is an incredibly irresponsible system with vast potential for misuse and by SPD's own data has extremely limited investigative use. Only .2%-1% of license plates can be tied to an investigation while the remaining 99%+ have nothing to do with an investigation and can be publicly queried. This is incredibly irresponsible and ineffective policing. I oppose the use of this technology entirely and find the data security policies laughably naive.
57	Ninety day retention of data especially for vehicles that didn't match any crimes at the time of scanning is a massive privacy violation. Other states require data on scanned plates that don't match to be deleted within MINUTES of the scan, not retained for months available to anyone. Members of the police force have regularly used data access for abuse of intimate partners for example, never mind people in the public doing PDRs and using the data abusively.
58	further increasing our dystopian police state
59	Police state invasion of privacy by a fascist, racist right wing institution we call SPD.
60	Privacy. This amounts to location tracking of most people who have cars
61	I have no concerns about the use of this technology
62	A publicly (or privately, given SPD's bad apples and their track records) database of all license plates, even those uninvolved with a crime that extends back three months is a massive privacy concern. SPD seems hellbent on acting as the security force for a futuristic dystopia where all members of Seattle society are tracked and traced "just in case". Not to mention this is what I imagine will be a taxpayer burden when the council just pushed through ShotSpotter. This kind of expansion of the SPD's power can only end in tears and bloodshed.
63	Retaining license records for all drivers even when unconnected to a crime is a severe invasion of privacy. Especially considering anyone can obtain the records. I dont want to live in a surveillance state.
64	Reasonable and trustworthy oversight of police using it
65	Overreaching surveillance with no warrant or due cause
66	I have privacy concerns that my data will be stored and mishandled.

67	Invasion of privacy
68	I am concerned that it will make everyone capable of being easily stalked and targeted, by government agencies or literally anyone. The domestic violence concerns alone are staggering. This will make it easy for abusers to stalk their victims. This technology will literally kill people when abusers can so easily track their victims.
69	No major concerns, I think something like this should have been implemented long before now.
70	I have significant concerns about the use of this technology and the way in which it could allow for tracking of residents. Data about where I go or frequent could be available as part of the public record and I'm concerned about lack of training and oversight on how that data is accessed or used. I live in a highly patrolled area and also think it could disproportionately collect the data of me and my neighbors compared to areas that have less parking enforcement or law enforcement presence. As a young woman, I'm also concerned about anyone being able to track my movement without my being aware of it.
71	This technology logs and retains information about license plates for far too long. This information should be purged immediately for plates not immediately determined to be connected to a felony or stolen vehicle. I'm concerned that the privacy implications of this technology and potential for misuse outweigh the marginal benefits that might come from recovering stolen property or resolving other criminal activity. I'm also concerned that this technology can be accessed by police and via public information requests. This technology should only be used by organizations with a high amount of public trust, and used in a way that does not degrade the amount of trust between citizens and SPD. That trust has been severely undermined between the public and SPD, and has warranted federal oversight of the department. Recent reductions of that oversight does not immediately increase the level of trust between the public and SPD. Eventual misuse of this technology (as with other police databases with documented abuse cases) will contribute to further erosion of trust between SPD and the public.
72	The ability for someone to access recorded location data from the last 90 days just by asking. why the fuck should someone random be able to know where i've been? do you not understand that this puts people at risk of abusive ex partners and enables stalking? Additionally, police officers should not be able to access peoples data when there is no evidence they have been part of a crime or broken any laws. this greatly increases the risk of abuse of the system by officers
73	Any increase in number of these surveillance devices must be met with far stricture retention rules. No non-interesting license plate data should be saved more than 48 hours PLUS department data access should require approval with reports on who requested access to what available to the public and media after a short amount of time.
74	It is a huge overstep for the police department and also opens up personal safety and security concerns for citizens. Anyone in the public can request info from the police department based on a license plate and use that info for things like stalking and harassment.
75	Surveillance tech doesn't make us safer. And SPD has no proven history of ethically and safely handling sensitive non-criminal data for even short periods of time.
76	The costs in terms of privacy invading surveillance are much greater than the perceived benefits. It's also a misguided approach to ensuring safety
77	The long length of time that passive data is retained and available to the public with no guardrails to make sure the general public safety is protected.
78	I am deeply concerned about expanding police surveillance over those who aren't even suspected of a crime. There is no benefit to holding this data on non-suspects, and many other states and cities use license plate recognition technology without storing non-criminal plates. There have already been documented abuses of this system by SPD officers.

79	The proposed expansion is an overreach and a big step toward the imposition of a surveillance state upon the people of the United States. The problems with this sort of expansion of surveillance have already been proven and well documented. The American Civil Liberties Union, digital privacy advocates, and researchers at the University of Washington's Center for Human Rights have raised concerns about keeping such detailed vehicle location information on people not associated with any criminal activity. Office of Police Accountability investigations give plenty of examples of how SPD officers abuse police databases. In 2021, an SPD officer used these systems to track his ex-girlfriend's new boyfriend. In 2020, an officer accessed information about an ongoing domestic violence investigation and possibly shared that information with one of the people involved. Early this year, another officer searched whether a suicidal family member had any registered firearms. UW researchers raised concerns about how ALPR data could be used by federal agencies to track undocumented immigrants or by other states to track those coming to Washington to seek abortions. Beyond what governmental agencies can do with the information, literally anyone can access this data through a public information request. Someone can request all SPD ALPR data from the last 90 days and if they know your license plate number, track your location. So, even if you believe in the trustworthiness of SPD, the federal government, or the protections Washington put in place sheltering people seeking abortions, you might consider whether you trust just an average person, or an ex-partner, to be able to request and access this data. This is all terrifying, and we the people are strongly opposed to this proposed regression in our liberty.
80	I am deeply concerned at the erosion of privacy, the expansion of pointless surveillance, and the already-proven harm potential for allowing poorly-supervised and unaccountable police officers access to information that allows them to track members of the public, even those involved in no investigation and no crime. This technology has already been seriously abused by officers who use it to spy on their intimate partners - those officers are still on the force, safeguards have not improved, and officers can rely on nothing more than a brief suspension even for serious betrayals of public trust. Lacking true accountability for misconduct, limiting police power is the only way to reduce harm to the community. Seattle Police have demonstrated, year after year, even under the consent decree, that their methods and tactics are abusive and disproportionately aimed at communities of color. This technology would kick open the door for increased dragnetting, improperly targeted investigations, and traumatizing stops of Black, Latin, and Indigenous people. I strongly oppose the expansion of this surveillance.
81	The police have more than sufficient means of surveilling people. This just reinforces their general tendency to treat private citizens as de facto criminals.
82	this technology would enable draconian surveillance by police department, who have a long history of abusing the people who live in this city. The SPD has historically abused access to private information that has been given to them, and faced very little repercussions. Giving them more spying technology will not make anyone who lives here safer, but will send a clear message to the police that the harm they do to the people that live in this city is fine and they should keep it up.
83	I'm concerned that through freedom of information requests, someone could track my whereabouts. I'm concerned that through internal access, government officials with personal reasons could track my whereabouts when I'm not associated with any crimes.

84	The police have generally proven to be irresponsible with public data and tracking, and I don't trust that they will be good stewards of this additional power and information.
85	This is a terrible violation of privacy. I understand the desire to automatically capture license plates in order to determine if a car is on a "wanted" list, but maintaining that data for up to 90 days for cars which are NOT on that list is a direct violation of privacy and a terrible idea. Bad actors can use this data in order to track movement of people (cars) in a scale that is dangerous. It is naive to think that not linking a license plate number to a person's DOL record will preserve privacy in any meaningful way, especially if a bad actor is targeting an individual (who they most definitely can find out their license plate).
86	I cannot overstate how concerned I am about this technology and how opposed I am to increasing surveillance to any degree on the people of Seattle. Tracking and storing this information is a huge a privacy violation by the city and its police department, and the proposed system additionally opens a wide gap for abuse. There are already documented cases of police officers abusing this system to stalk people in their personal lives, and collecting and storing more data only enables this further. In addition to abuse by the state and police officers, the fact that this information, which should not be collected and stored in the first place, is publicly available, means that anybody with ill intent can track a person or people's location. To state it clearly, I am strongly opposed to this surveillance technology, do not believe it should be adopted at any scale, and in fact believe that it should be removed from the vehicles that already have it.
87	"ALPR data is gathered indiscriminately, collecting information on millions of ordinary people. Law enforcement agencies have abused this technology. Police officers in New York drove down a street and electronically recorded the license plate numbers of everyone parked near a mosque. Police in Birmingham targeted a Muslim community while misleading the public about the project. ALPR data EFF obtained from the Oakland Police Department showed that police disproportionately deploy ALPR-mounted vehicles in low-income communities and communities of color. In 1998, a Washington, D.C. police officer "pleaded guilty to extortion after looking up the plates of vehicles near a gay bar and blackmailing the vehicle owners. Police officers have also used databases to search romantic interests in Florida. A former female police officer in Minnesota discovered that her driver's license record was accessed 425 times by 18 different agencies across the state. In addition to deliberate misuse, ALPRs sometimes misread plates, leading to dire consequences. In 2009, San Francisco police pulled over Denise Green, an African-American city worker, handcuffed her at gunpoint, forced her to her knees, and searched both her and her vehicle—all because her car was misidentified as stolen due to a license plate reader error." Source: Electronic Frontier Foundation https://www.eff.org/pages/automated-license-plate-readers-alpr
88	The use of this technology has already been abused by SPD officers for personal matters; why in the world would you expand it? More cameras are not going to solve any issue with crime, and you are deluding yourselves if that's what you believe.
89	Privacy. Non-hot-list records should not be retained at all.
90	Privacy, abuse of information by the police.
91	This technology is a blatant breach of our right to privacy. This data has been used for illegal tracking of citizens by the government & police, & can be used by private citizens to track one another to a dangerous degree.

92	My concern is how it will be used against innocent citizens. There are instances where it has been used unethically and human behavior when surveliance like this is available will make this hard to control.
93	It's and invasion of privacy , its a form of predator stalking SPD is not a trust worthy organization Civilian's can access this same information and that is dangerous
94	Where will the data be stored? Any member of the public can access this data. This opens people who have stalkers up for abuse. What about the domestic violence victims?
95	I have many concerns: first of all, how is the data going to be protected so it can't be tied to people? Also, if other departments can delete the data instantly, why can't SPD do it and why do they have to have it for 90 days? Why is so much of privacy...about parking enforcement, what does outweighs the violent crime reduction for asking the entire city to give up privacy? Most of the people with parking tickets/parking enforcement are poor, people of color, and are policed disproportionately, this would just recreate those systems, and create even more disproportionate policing towards poor people/bipoc. How will SPD make sure the data is not used by ICE? Seattle is within 200 miles of a border...it says only officers who are trained how to use the automated license plate readers will have access to this info, but also, it says every SPD officer will be trained to use it...so basically the entire fleet, this is contradictory.
96	This is an inexcusably invasive violation of every citizen's right to privacy. We do not deserve a police state with active government surveillance. This puts each of us at risk of falling victim to stalkers and domestic terrorist groups. SPD has repeatedly shown themselves to be untrustworthy with public data. This will rob funding from necessary community services without providing any public benefit.
97	I have concerns about the fact that this technology will save license plate data for 90 days, documenting days, time, and place that is accessible by any police officer, or anyone through a public records request. That is a privacy violation. The vast majority of people are not committing crimes on the road, collecting and making available this data to the public could easily be abused by people. An ex partner could use this data to track someone, an abusive family member could use this data to track.
98	Mass surveillance and invasion of privacy for no concrete benefit. Massive cost to the taxpayer with no guarantee of additional safety.
99	This will make things even more dangerous for victims of abuse and dv!!
100	I agree with all of the concerns here: https://www.thestranger.com/cops/2023/12/05/79293457/seattle-police-department-pitches-dramatic-expansion-of-vehicle-surveillance It's too invasive. The plates that are fine should be purged right away like other cities do. Or not saved at all, just run the plates against the list and only save plates that are a hit.
101	I am seriously concerned about warrantless and irresponsible searches of civilians. Given that at least 40% of police officer families experience domestic violence (https://olis.oregonlegislature.gov/liz/2017R1/Downloads/CommitteeMeetingDocument/132808), the likelihood of this tool being misused to harass and abuse innocent women and children seems high. Also, considering that the only accountability mechanism seems to be an internal review, I don't expect many officers to face significant consequences for inappropriate or illegal use of this technology.
102	This technology is extremely concerning to me. The implications for personal privacy far outweigh any investigative benefits of this technology. Complaints have been made about SPD officers misusing this technology which is a great concern. I do not believe this techology will be beneficial for keeping us safe in Seattle and will only contribute to the continual eroding of our privacy by expanding surveillance.
103	Stalking! If anyone can request the license plate info for any time for 90 days, so many women will be at greater risk of domestic violence.

104	No concerns with this technology. Driving a 2-4 ton car/truck is a privilege and should be treated as a privilege with no expectation of anonymity. Especially given the horrific damage they cause and the ability to use them ways that put others at risk and subvert the law. Cars need to be monitored as drivers are often awful. Poor drivers compel SPD to use Automatic License Plate Readers (ALPR), which take pictures of license plates and records the date, time, and location of the plate. If someone wants to be anonymous then they shouldn't be driving.
105	It will be used to violate privacy, regardless of claims by SPD. There are no safeguards in place.
106	Rampant privacy violations both by the PD/city and the general public through FOIA requests.
107	None; I encourage it.
108	The use of this technology, if at all, should be strictly limited to reading license plates that are known to have been associated with a crime. The wholesale collection of this data and 3 month retention is a blatant invasion of privacy and power grab by a department which has proven time and again to be corrupt, fraudulent, and dismissive (at best) of constituents' best interests.
109	I don't like the idea of tracking all vehicles even though they are not connected with any criminal activity. Too Big Brother
110	It violates privacy rights
111	There is little public benefit to mass surveillance, and it comes with a significant public cost in terms of potential for violations of privacy. Just one example: a system like this would enable officers with malign intent to better track the location of estranged partners and enable stalking.
112	This is a grave violation of personal privacy.
113	I don't want cops or trolls to have more tools with which to bully.
114	This is going to make it so that people can see plates of women fleeing red States to access what should be perfectly legal care, & is in our state, but not theirs. This will put 1000's of vulnerable women at risk.
115	I have many concerns about this technology. Seattle has repeatedly shared their absolutely distrust in SPD, and having a tool like this will only further cement the lack of trust. The people of Seattle deserve to walk around their city without feeling like they're watched by the city/SPD. This technology, as many things implemented by SPD, will be used as a tool for discrimination against BIPOC and houseless folks. This technology makes Seattle feel much less safe and welcoming.
116	It is a gross abuse of policing and via surveillance and will only serve to gather data that is either worthless or ripe for abuse. So the only people who will benefit from it is those seeking to abuse it.
117	Several concerns. Perhaps if the ALPR was limited to only being used to check against "any license plate numbers that have been uploaded into the onboard, in-vehicle software system," as described in section 1 of the ALPR Executive Overview, the invasion of privacy would be a reasonable trade off. However, it doesn't do that. It stores the data it gathers for 90 days. The cited reasons for this technology is for stolen cars and Amber alerts. How is retaining this information that one would need to act immediately on for 3 months a good idea? Having that data stored so long also opens up other issues. Even leaving aside the issues of SPD employees having access to this database and using their credentials to search out things personally relevant rather than related to their cases, as has already happened, there is still the greater concern of sharing with other law enforcement agencies. Washington has become a haven for those seeking abortions and otherwise exercising their reproductive rights, but this is increasingly illegal in other states. 90 days of retained footage for more and more records of license plates sure seems like a lot of information that could lead to the persecution of people in their home states.

118	My two main concerns are 1. The fact that SPD can not use or purge the data in a timely fashion. What is the point of collecting it in real time if you can't use it quickly? At what point does the gathered information become useless since the vehicle is long gone? Why does it take SPD longer to use and purge than other jurisdictions? It seems like there is inefficiency in the SPD if they can not gather and respond like other localities can and adding more data to the mix will only bog things down. It is a waste of money, resources, and time, especially when considering that the use of the data does not significantly increase the crime solving rates. 2. The information can be requested by the public. There are inherent risks with allowing this data to be accessed by public entities. The move to a surveillance state is concerning, especially with all the current uncertainties with civil and healthcare rights. The fact that other states have laws regarding women's healthcare that can bring civil suits and jail time, the ability to locate and monitor persons moving around in WA state is a HUGE privacy issue. Racial, gender, and sexual tracking is a real concern. Knowing that there are "bad actors" that will use this information for their own purposes, and also knowing that the technology does not provide a significant amount of benefit in helping to solve crimes, it is only useful to those that want to track and surveil others. In addition to my main concerns, the costs of installing and maintaining this technology could be used in some other capacity that would be more useful. Training, recruitment, etc are some areas that come to mind. The only benefit would be that the officers don't have to do anything while driving around.
119	If this database is made public, stalkers and abusers will be able to search for their targets by license plate, identifying their locations at certain days and times, even if they don’t know the person or know their name. This is an obvious increase in risk and danger to the public.
120	This expansion is a solution in search of a problem, since the # of license plates identified with a crime is less than 1%
121	I have MANY concerns about the use of this technology. SPD has already had numerous, documented incidents of police misconduct around license plate and other surveillance technology — this tech would only expand the abuses of power. The privacy and civil rights infringement is too much to bear. As a Seattle resident/voter/worker, who comes from communities most targeted by these kinds of surveillance, I absolutely oppose this tech being used at all, much less expanded.
122	Overreach. Data Retention FAR too long. Massive cost with no ROI. Stalking (by Police AND Citizens) Mission Creep (always happens). Data Security which has been stated will not exist.
123	This technology should be prohibited; ALPR retaining data is a significant privacy violation even in its current limited use. Dramatically expanding the use is a terrible idea that will result in less privacy for millions of people. This program should not be expanded, and data should be purged immediately. Even without abuses by the Police department, the availability of this data via public records requests makes it extraordinarily troublesome.
124	I understand and appreciate the benefits of running plates to catch felons and recover stolen cars. What I object to is being subject to constant surveillance with my location logged in a database for 90 days. If the police has a list of stolen plates, it's fine to scan for them at the time of capture (or at most, within a day). The database is the problem. I cannot be free and safe in a city that tracks and logs my movements. That's dystopian and scary. It would be a dangerous violation of our privacy.
125	None

126	Misuse of data, tracking of individuals based on their license plates for non law enforcement activities. The very small percentage of data that is at all useful to law enforcement, compared to the large amount of harm that could be done to someone in an abusive, controlling manner.
127	Privacy violations, misuse, data breaches.
128	All concerns. Concerns for those who are being stalked, concerns for those who have dealt with domestic abuse, and concerns for anyone. This technology is unethical, and police do NOT need this data. I don't think infrequently about how this data may even help cops - who, statistically, commit domestic abuse at much higher rates than the general public, stalk their own former or current partners. This is a privacy and ethical violation. If this is signed off, you can guarantee that none of the co-signers will have my endorsement or vote moving forward.
129	ALPR devices present significant privacy and equity concerns while showing little efficacy in reducing crime. For specific civil and human rights threats posed by this technology, see a 2022 report by the University of Washington Center for Human Rights, "Who's Watching Washington?" https://jsis.washington.edu/humanrights/2022/12/07/whos-watching-washington/
130	tracking civilians will be abused, waste of money
131	It is overreaching and would document the lives of those not suspected of crimes which is a violation of our rights as US and WA citizens.
132	Seattle Police has a long history of a use of power, keeping data on non suspect vehicles more than 48 hours is unreasonable and should be banned!
133	I worry about the overuse of public surveillance posing more risk to people than helping them.
134	The local publication The Stranger explains my views on this issue : “However, SPD also retains license plate numbers that don’t register as a “hit” on the hot list. Given that ALPR can collect tens of thousands of license plate images in 24 hours, and that SPD would roll out the technology to all of its patrol cars, officers have a high probability of capturing an image of the average plate at some point. Photos of those plates, as well as the time, date, and location, go into a database and SPD keeps that data for 90 days.” This is a massive surveillance issue and is unnecessary. You should focus on working with community orgs and not wasting your funding on technological surveillance! The ACLU of Washington has also noted similar issues with this technology. Instead of spending money on this tech, you should train your officers better so they don’t run over and murder pedestrians, and then make poor jokes about it after!
135	There are insufficient controls over this data to ensure that it can't be abused by SPD personnel, divulged inappropriately to third parties including members of the public, or accidentally leaked. This would never pass muster in any corporate data compliance discussion, as this represents linkable information that has significant privacy implications (even outside the hands of law enforcement) that merits equally significant safeguards that do not exist in this proposal. Those protections must come first.
136	I would want to make sure that the public that requests information is tracked or vetted. Could someone use the public request to stalk their girlfriend? (Also wouldn't want the police to use the tool internally for non-case related things, so would track who checked what and when)
137	Data retention, even for 90 days, introduces the risk of the records leaking or being improperly accessed. That access could be used improperly to stalk or harass drivers who are observed this way. One example is a spouse of a police officer whose plate might be scanned near a medical facility or a lawyer's office without their spouse being aware.

138	Serious privacy concerns. If anybody can trace someone's movements this exposes people to danger from stalkers and abusive ex partners. The police have no need to keep this information and it is a severe breach of citizens expected right to privacy
139	This is a terrifying expansion of government surveillance well beyond any reasonable grounds. Creating a mechanism to track individuals, especially those who are completely innocent, is a threat to the safety of our people and democracy. There are countless examples of perfectly legitimate actions that could lead to harm if they were tracked. Some states are outlawing abortions, including people who get out of state abortions. This data could be abused by those governments to prosecute their people. It could also be used to track protestors, etc. It could similarly be abused to stalk someone, etc. This abuse could happen either by someone with inside access, or someone performing a FOIA request. It's a massive invasion of privacy. It also sets the norm for this, and makes future decisions easier to justify, because they're already doing it here. We need to stop it before it happens.
140	I don't have any concerns
141	SPD has a documented history of misuse of the license plate scanning technology, this will only become more likely as the data set grows. The proposed limitations and restrictions have not, and will not, be sufficient. Lastly, the problem space supposed to be solved by this is dubious at best, it clearly can't prevent or reduce crime. The budget allocated to this would he far better spent on supportive housing and other community initiatives shown to actually prevent and reduce crime.
142	This is a violation of privacy. At a minimum, require deletion of the data within minutes as soon as there is no relevant match.
143	This technology violates every person's right to privacy provided under the US Constitution. In the strongest way possible I urge SPD that NOT impliment this policy.
144	Foremost that we cannot trust SPD to use this data effectively or fairly. SPD has been under a consent decree and has proven again and again to use racial bias and discrimination in their policing. This tech will not change that, and just be one more thing for SPD to abuse! And in general is my concern about privacy and the fact that we are becoming more and more surveilled. Surveillance does not make us safer or reduce crime, that's a fact. Let's use this money to invest in the community in ways that are proven to increase safety.
145	This is too great an infringement on privacy, given the expansion of the technology to so many vehicles and the retention of the data for 90 days.
146	this surveillance technology will cause more harm than it will do good. instead of more resources going to surveillance, why don't we invest resources into things people actually need, like housing, social services, medical care, etc? as a community member in seattle i am completely opposed to this technology.
147	Why does the department need to keep the data for 90 days when other jurisdictions keep the data for only minutes to hours? What protections do you have in place that prevent abuse from employees that can access the data? Why should we trust that the information can't be used against civilians by other civilians through the public information request process considering this information would otherwise not be available for such an extraordinary amount of time. Aren't you effectively presuming guilt by saying the 90 days is required to determine whether you have captured a significant image?
148	None
149	None

150	It will lead to false positive and more shootings by the police of unarmed youth.
151	I worry SPD officers using it to illegally surveil family members, spouses and anyone else they are interested in for personal reasons. Even other police officers they suspect might report them. I also worry the technology makes a mistake and I am pulled over for no reason, thus putting my life at risk
152	I feel that this technology should not be pursued. The data retention period for "non-hits" is too long and is subject to data breach events, public disclosure requests, and misuse by SPD staff, which has already occurred and been documented with the existing ALPR fleet.
153	We live in a police state already and the cops are known to be abusive. This opens up more opportunities for cops to be abusive. This isn't going to have tangible effects on public safety. It will just strengthen the watchful eye of the police state.
154	Massive privacy overreach for those who haven't committed crimes. Police abuse of database of information.
155	I am against the use of this technology. Per the U.S. Court of Appeals for the D.C. Circuit in a GPS tracking case, United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts." Such technology is anathema to both our innate and legal freedoms, and I urge city council to stand up to the military-police-surveillance-industrial complex and reject its use.
156	Even your own employees can't be trusted to properly use this data and not use it for their own purposes like stalking people they don't like, and you expect the public to wisely use the license plate information? No. Don't store the plate data if it's not linked to a known crime, and definitely don't make it publicly available.
157	I am concerned that it will capture data that is private, and make it available to third parties with no legal interest in the data. Per The Stranger, "not only do cops have access to that data, but anyone can request the database of license plate photos and numbers along with the time, date, and location of when SPD took the photo. A lot of cities purge this data quickly if the plate doesn't match a "hot list." SPD gave no real explanation for why it couldn't purge the data..." [Though I also see that the ALPR report at seattle.gov states that only properly trained employees will access the data, which I hope is true.] I don't understand why this technology--which apparently captures data at least 98% of which is unrelated to any crime--is necessary, and I certainly object to its use to retain said data for months on end. I am not sure how the restrictions on its use, the specific deployments listed in section 2.0 of the ALPR report, can be monitored and enforced. I would like to know how demonstrably useful the technology has been in its initial deployment, and whether restrictions have been observed. I do appreciate the opportunity to comment.
158	Privacy, abuse of power on the part of police
159	I'm concerned it will increase police power, increase police contact with the public, and increase police killings. I'm concerned about my privacy.
160	This technology invades one's privacy and makes spying on one's neighbor possible.
161	Data shows us that law enforcement officers commit domestic violence offenses at high rates, allowing them the ability to track the locations and daily habits of people seems like a good way to let abusers keep tabs on their victims

162	I am concerned about retention of license plate and location information that is then subject to public disclosure to private investigators and private citizens with their own agendas. Two cases illustrate unwanted consequences: 1) Disclosure of this information could enable identification of women who have crossed into washington state for abortion access. Laws in other states are now criminalizing the transport of a woman for an abortion out of state. License plate and location information would facilitate prosecution of such women and those who assist them, inhibiting exercise of women's rights to protect their health and make reproductive choices. 2) Disclosure of this information to private investigators working for long-term disability insurers would further weaken protection for the disabled who have paid for insurance benefits. ERISA laws set a very low bar for disability insurers to deny insurance coverage to the disabled. Although washington state laws now provide a "de novo" courtroom standard for proving disability in some cases, this still does not apply to self-insured companies, who are still granted a "deferential" standard under ERISA in washington. This means that the insurer can deny insurance by merely muddying the waters on a disabled person's capabilities for employment. The do this by having a PI observe the insured doing ordinary things (e.g., going a grocery store), then claim that this is proof of employability. A database of license plates and locations would give them vastly more fodder for specious denials. It costs tens of thousands of dollars to disprove such specious claims, money that few disabled people have in ready cash. It is also costly in distress and time that disabled people need for medical care and rehabilitation in the hope of return to employment. Further, many disabled people get so discouraged by insurer and PI shenanigans that they do not fight for their paid-for benefits. Few know how to do so, or have the physical/mental/emotional/financial wherewithall to do so. Rather than believe my citizen's report, please contact an ERISA disability attorney and ask what they think PIs for disability insurers would do with publicly available location and license plate data. In case you are not familiar with ERISA, I'm referring to long-term disability coverage provided as part of group insurance plans to employed people. Generally employed people pay the premiums to protect themselves if they are incapacitated by disease or injury. I'm not talking about social security disability. Please consider the most vulnerable people. Please ensure that data retention is so brief that any public request for data is so unlikely to return an individual's license plate that a PI or abortion activist will not bother to request it. Do not give their people another tool to use against the vulnerable. Please consider this both for any existing technology already deployed, not just new technology.
163	This is a breach of privacy
164	This is inappropriate and unnecessary. A violation of the public’s privacy and allows for cops without good judgement to further discriminate against mainly marginalized groups populations
165	I am concerned about the general privacy risks associated with storing vehicle location data for several months. I do not believe that citizens’ personal information (daily whereabouts) should be accessible to police without the police having good cause for needing that information prior to collecting it. Even if you are suspected of a crime, I believe there is information that could be gleaned from your day to day location that should be kept private for reasons of basic human dignity, especially if an individual officer’s judgment is the only barrier to accessing that information. Collected data should be filtered down to only that which is strictly necessary and beneficial over traditional police work, should be stored for as little time as possible, and should only be accessible in formats that answer essential police questions (eg, last known location vs location history). If technical constraints are cited as a reason for the current plan, more technical research, consulting or experimentation is certainly warranted given what is possible in plenty of other high scale software systems. Concern should also be noted for the general security risks associated with storing this data, which is sure to be a target for attackers who might profit from selling it to bad actors.

166	This is a dream come true for stalkers and abusers. A public registry of locations of specific license plates, in which the SPD is not committed to purging noncriminal plates? What an easy way to continue victimizing anyone with a car! Keep in mind as well, that police officers themselves are far more likely to commit domestic violence compared to the general population; it's downright dangerous to their victims to give them free access to this kind of data. This also creates a loophole that allows, for instance, employers to get information about employees' health status that they are not legally entitled to. Why should employers-- or anyone, including police-- have the data to see that someone parks at the time and place of an Alcoholics Anonymous meeting, or at clinic offering abortion services, or an AIDS or cancer survivors meetup? All they need is the license plate number, which many can easily get when an employee parks at their workplace (or even shows up for an interview-- what a convenient way to maneuver around hiring discrimination). This is before considering the truly terrifying thought of the number of innocent people who will get pulled over and guns drawn on them just because a software misread a "1" for an "I".
167	This increased surveillance is intrusive to the daily lives of people in Seattle and is not even effective at addressing real harm if less than 1% of plates are connected to a crime. This puts too much power in the hands of the police, which have time and again shown they will abuse this power. This violates the privacy of individuals, and I worry about this being used to track people seeking abortions in Seattle from out of state. Additionally, if individuals are able to publicly request these, this is directly harmful to people especially in cases of domestic violence.
168	Invasion of privacy
169	The technology is a MAJOR privacy issue and there are not any parameters on its use and disposal of the pictures. SPD has abused this technology in the past and no constraints are in place to contain the abuse.
170	first ammendment
171	As a member of the state address confidentiality program (ACP), I am concerned that such a technology could be used to track my location for the past 90 days through a public records request without my knowledge, even though I am not under investigation for any criminal activity.
172	Overreach of power - capacity to track movements and retain info on people - high cost of this technology when there are other pressing needs/ social services that should be funded - the potential for abuse of this data by police - the potential for abuse of this data by other than police - I oppose increasing surveillance of people going about their day-to-day lives.
173	It is an illegal invasion of privacy when random collection of license numbers includes non-criminals and is kept for 90 days.
174	This is a massive privacy violation. This is surveying the public without their consent and should not be tolerated. Without civilian oversight on how the data are stored and accessed, I am very very concerned about the amount of data and power this will provide SPD
175	When considering the adoption of any new technology, law enforcement related or not, we must think about how bad actors may use the technology to harm the average person or target individuals. With the potential list of abuses including stalking, harassment, unreasonable surveillance, and violation of privacy — combined with the potential positives of only 1-2% of plates actually being linked to crimes— implementing this technology does not pass the test. The people of Seattle would be better served by public services that improve their wellbeing and raise the quality of life than giving the police more tools with which they can surveil the public.
176	This an extreme breach of public trust and the right to privacy for the general population. This technology, if used at all, needs to be limited. Data from this technology needs to be analyzed and non-hit data needs to be discarded

	rapidly. The SPD's excuses of being unable to delete images within even 48 hours when other departments and districts across the United States can do so within minutes goes to show how this technology can not be trusted in the hands of SPD. By collecting this data and holding it for months at a time and allowing it to be publicly available opens up more concerns with our current constant surveillance state and growing over-criminalization of daily life. Do NOT allow this data to be kept for 90 days.
177	Privacy, privacy, privacy. The retention period for this data is far too long. There is no reason to hold onto this data for 90 days, or really at all. In fact, there's no reason to retain the data at all. Rather, you should push license plate of interest to the ALPR systems in the field. They can alert when they find a plate of interest and drop all other plate and location data that is not of interest.
178	That it will be used to further criminalize minoritized communities
179	This will further escalate police violence and racism and targeting of vulnerable individuals, as a social worker this is unethical and will hurt the clients I serve and the people you claim to protect but actually just want to control.
180	Violations of privacy of everyday citizens. If this technology were to be adopted, it MUST be set up to purge its database of non- "hot list" license plates within a very short amount of time, one or two days max. I'm largely concerned about the ability of the state to track the movements of private citizens who are exercising their constitutional rights. Access to such information has historically always, always been used to subvert the rights of members of marginalized communities.
181	That ALPR can collect tens of thousands of license plate images in 24 hours, and that if SPD would roll out the technology to all of its patrol cars, officers have a high probability of capturing an image of the average plate at some point. Photos of those plates, as well as the time, date, and location, go into a database and SPD keeps that data for 90 days and can be made available to the public.
182	The concerns for the proposed use of this technology are almost too numerous to detail in this form, but I'll try to summarize. This technology and the proposed scope of collection and storage time for images puts thousands of innocent civilians at risk. First, victims of domestic violence can be located and tracked by disgruntled (and possibly violent) ex-partners simply by knowing one's license plate and filing a public information request. Victims of stalking can be similarly tracked even after moving. Washington state, and Seattle especially, is established as a safe haven for women seeking critical reproductive care. Other states, including Idaho, and radical anti-abortion groups have made clear their intentions of harassing, doxxing, suing physicians, and prosecuting women leaving their states in search of this potentially life-saving medical care. There seem to be no safeguards in place to prevent agencies in other states or random Washington residents from accessing these records. Given the proposed breadth of installation on SPD cruisers, anyone with a vehicle parked outside of a garage is at risk of these outcomes.
183	The proposed level of surveillance is a massive invasion of privacy and a security threat to all Seattle residents. The data that are not linked to a crime should be purged within 3 minutes as in New Hampshire. The data should not be a public record that can be used by criminals to target innocent citizens. The data has already been abused and the risk is only growing with the proposed expansion of the ALDR surveillance
184	This technology represents a gross encroachment on the right to privacy and presumption of innocence.
185	These technologies create a pervasive state of surveillance that is easily abused, and perpetuates an adversarial relationship between police and the public. The burden of proof that a technology is having a positive impact on safety must be exceptionally high to warrant broad collection of data. In this case, if the technology is adopted, at a minimum the retention time should be minutes (as it is in other places), not months (as is proposed).

186	I am very concerned about the use and expansion of ALPR technology to 300 police vehicles. Passive data collection that can lead to tracking an individuals movements by both police and the public through records requests is a danger for everyone, and especially people with stalkers, women in general, and marginalized groups already disproportionately targeted by the police. Building this database of peoples license plates who just pass by a police vehicle and without knowing their data is being collected/stored in this way is a major privacy violation and further severs any sort of community trust in the police. Allowing this expansion also paves the way for even more dangerous automatic and AI-assisted surveillance technologies that might do the same passive data collection, using facial recognition etc, and again actively making the general public less safe and collecting personal data without the persons consent. Waste of city funds to expand this technology's use.
187	I'm concerned about the expansion of surveillance of everyday citizens who pose no threat to community safety. I oppose the further militarization of police forces across the country and am deeply disturbed by this practice being funded, implemented, and expanded largely with money extracted from the very civilians you wish to "track" through tax dollars. I refuse to pay for my own surveillance and the surveillance of everyday citizens.
188	Data gathered by state and local law enforcement is accessible to both law enforcement from other states, and federal immigration enforcement agencies, through interoperable databases. Research has shown that by tapping into vast reservoirs of personal data offered up by private data brokers, ICE is able to effectively bypass 'sanctuary' cities. While law enforcement claims to be using this data to solve violent crime - even promoters of this technology admit that only a small percentage of scans—typically less than a fraction of one percent—turn out to be relevant to public safety concerns. The ACLU estimates that less than 0.2 percent of plate scans are linked to criminal activity or vehicle registration issues. SPD claims their primary concern is to stop crime and disorder. How can they possibly claim this when 0.2 percent of plate scans are linked to criminal activity. Especially because this license plate information would be available for 90 regardless of whether or not the license plate is connected with any crime - I worry about how it might be used by immigration officers, might be used by law enforcement from states that have outlawed abortion to track individuals traveling to Washington, might be used by violent domestic partners or stalkers (as this information is available to the public with a public disclosure request). In August 2012, the Minneapolis Star Tribune published a map displaying the location, obtained via a public records request, of the 41 times that Mayor R.T. Rybak's car had been recorded by a license plate reader in the preceding year. In these times of political vitriol it is not inconceivable that this technology could be used for nefarious purposes. ALPR data is gathered indiscriminately, collecting information on millions of ordinary people. By plotting vehicle times and locations and tracing past movements, police can use stored data to paint a very specific portrait of drivers' lives, determining past patterns of behavior and possibly even predicting future ones—in spite of the fact that the vast majority of people whose license plate data is collected and stored have not even been accused of a crime. I fear this will could used to curb first amendment rights. Bumper stickers can even be seen from the data collected. Police officers in New York drove down a street and electronically recorded the license plate numbers of everyone parked near a mosque. Police in Birmingham targeted a Muslim community while misleading the public about the project. ALPR data EFF obtained from the Oakland Police Department showed that police disproportionately deploy ALPR-mounted vehicles in low-income communities and communities of color.
189	The increased number of ALPR installed and used in SPD patrol vehicles poses risks to citizen privacy, including increased opportunity for institutional abuse, discriminatory targeting, and tracking of individuals who are in no way associated with the criminal activities this technology claims to prevent or reduce. Additionally, as the data on license plates and citizen tracking grows, so does the incentive for private companies to purchase this data and use it for capital gain, or for malicious hackers to steal this data for the same end. The risk of citizen privacy loss is too great when compared to the value of this technology in investigating criminal activity.
190	I have major privacy concerns for all residents, including increase in surveillance of human rights activists, increase in stalking, increase in racialized arbitrary police stops, and personal information to be shared on a broad and not very secure network that is highly hackable, racial profiling and increase in access to otherwise confidential information. This technology is harmful to all and does not prevent any crime or increase community safety in any way. This is a major overreach.

191	The use of ALPR technology is a violation of privacy and safety. SPD officers have a proven history of abusing their access to this tracking information, and should not be trusted with such revealing info about civilians. To store ALPR data for 90 days provides ample insight into any vehicle's patterns and makes it all too clear what its driver or passengers are likely up to. It is unsafe for this data to be in the hands of cops, and it is unsafe for this data to be available to the public. SPD's desire to gain power via increased surveillance is unethical and is not sufficient justification for the use of this technology.
192	Firstly as SPD admitted some of the data collected can be used to track peoples location across the city. I do not want any government to have the capability to track the population on mass. Due to a long history of similar data being leaked through data breaches or whistleblowers informing the public of data about them being stored unnecessarily and being used to track civilians I do not have faith that this data will be used properly. It is not appropriate nor will it ever be appropriate for the government to set up systems that can be used for mass surveillance.
193	I feel it is a violation of our privacy. If we have not done anything wrong, why should others be allowed to look up information that is personal and private. This is like "Big Brother" doing anything they want to a citizen with no reason
194	Inability of community to access info when necessary and misuse and access of info by unauthorized LEO/FOP and other supporters/promoters of tech in LE. Like bodycams, resisted at initiation and manipulated when suited.
195	The Seattle Police Department have demonstrated repeatedly a racist bias, leading to the decade-long federal review commencing from 2011, the repeal of the bicycle helmet law because it was being enforced disproportionately to Black and other darker skinned people, in addition to the murder of the likes of Charleena Lyles, John T. Williams, and more. Allowing this sort of technology will only give more tools to the SPD for intimidation of non-white communities.
196	Vast overreach of the surveillance state. Let us fucking exist without tracking every one of us. Especially with SPD officers having been found culpable of grooming, tracking their victims using police resources, and more -- this is TERRIFYING as a woman who lives in the city.
197	This is an extreme violation of privacy that will do more harm than good.
198	This technology is invasive of the privacy of residents and visitors to Seattle. The records it generates can be abused by anyone who gains access to them, by any means.
199	I am a technologist who is deeply concerned about the privacy impact of SPD's proposed expansion of ALPR technology and strongly opposes any plan that increases the use of ALPR systems. Under SPD's proposed use, this ALPR system indiscriminately captures and stores the locations of innumerable vehicles, and by proxy their owners, the overwhelming majority of which have not been implicated in any crime. The public benefit of ALPR systems is dubious, and when weighed against individuals' rights to privacy, indefensible. The location information is liable to be abused by both authorized and unauthorized actors, and on the whole, a huge liability for the City of Seattle's government.
200	Storage of license plate data is too ripe for abuse.

201	I am concerned about the massive expansion of violation of people's civil liberties while driving in public that is presented by possible implementation of ALPRs. We have a right to move freely in public without being surveilled by law enforcement. It's also deeply troubling that data collected via ALPRs is available via public disclosure for such a long period of time. It makes no sense that other jurisdictions around the country can determine whether an image needs to be kept in only a few minutes and SPD is saying it takes them more than 48 hours and up to 90 days. If the system being acquired doesn't do automatic processing that would exclude images not of interest to law enforcement, this is also a bad investment for the City. It means that officer resources must be being used on evaluating images - with SPD understaffing as it is, it makes no sense to waste resources on this when there are much more urgent needs to attend to.
202	Mass surveillance. This technology scans and records the identification information of thousands of people a day, including geographical location of people who are involved in their day to day lives with no criminal intent and retains that information for 90 days. Further, it compiles it all in a database that is available to public records requests. This is a huge violation of people's rights to privacy in their daily lives. The right to personal privacy overrides any thought to the potential of "precrime." Having geographic and time information can expose a lot of information about people, from if they're cheating on a significant other (not a crime) to if they are going to a doctor's appointment. As abortion rights are under attack across the country, people traveling from out of state to receive needed healthcare should not have the added worry of their license plate information stored for long periods of time in a database that can be accessed by people in other states that are hostile to the medical procedure. Furthermore, this creates a potentially disastrous situation for people in dangerous situations such as domestic abuse or stalking. If anyone can access this information, even if protection orders are issued, there would be no way to stop a third party from potentially accessing the information and passing it along instead.
203	The capture and storage of license plate information is an inappropriate use of police vehicles. The capture and storage of license plate information in a form available to the public is an irresponsible use of police vehicles. Most surveillance technology is useful and helps someone do their job. That this would be useful is not special. What is exceptional is that this would fully enable the public to repeatedly request this data as a public record in order to construct a long-lasting open repository of vehicle data. Anonymizability does not change the appropriateness of this choice. If I have a record of this kind, I can extrapolate public behavior to a degree that no citizen should be able to access. When we look at whether someone should have access to data, we must ask under what circumstances they would otherwise be able to gather it. In this case, the answer is a network of community vehicles with cameras, license plate readers, and a collectively pooled repository of image data. It would be uncomfortable for the average citizen to know that their neighbor was constructing such a system. This technology effectively constructs such a system for all of my neighbors.
204	Stored information of people who have not committed any crimes could be misused by department of public access.
205	I'm concerned about the massive amount of publicly-available data on driving habits, locations, and vehicle information being available on 3-month rotations. I do not trust SPD to keep the information secured.
206	I am all the way against this this violates our civil rights and takes away some of the few freedoms that we actually have left in this world this violates the very Constitution that our country was built on and in no way is this okay or Fair
207	It’s incredibly privacy invasive, and the retention of data for such a long period of time is extremely ripe for abuse. There’s no reason license plate and location data needs to be retained any longer than for a computer to check whether the license plate matches a list of persons of interest.

208	Infringing on privacy. It is an overstretch. And we have seen when technology is in the hands of people with power that it is abused. Every time
209	Waste of budget. Infrindging on privacy.
210	The use of automatic plate readers is a huge privacy infringement. When made public through public record requests, the information becomes even more of a privacy concern.
211	Police surveillance is bad. Police mainly exist to repress activists so the less information they have the better
212	Privacy, safety and security.
213	This is an infringement of civil rights and protection against illegal search and seizure
214	The people who live and work and drive through our city would be subject to passive surveillance. Those who drive frequently, such as for blue-collar delivery jobs, would be disproportionally impacted. Data, once collected, is subject to abuse, especially in the hands of SPD. There is not a need for this and it is a huge waste of taxpayer money.
215	All of them. This is a disgusting use of technology to infringe on people's right to privacy! Give us a database of all cops to track in real time and then MAYBE I'll consider not hating the guts of each and every individual pushing for this. Just maybe.
216	This is a violation of privacy and I'm deeply concerned about the ways location tracking will be used to harm people in the community, by both law enforcement and other community members (esp in stalking or domestic violence situations). This is such a waste of city money and there are other actually helpful things that our city should be investing in - housing, healthcare, education, community groups.
217	That SPD will not delete the findings soon enough. No need for spd to hold unneeded license plate numbers. Also studies show that it may detect very few license plates that have been involved in crime. Appears to be a lot of $$ with little benefit.
218	I am concerned that this will increase surveillance of poorer communities and result in more policing for people of color.
219	I am concerned that this information will be abused by members of the public to harass and target community members. Because the database is available publicly, the 90 day retention policy will be easily bypassed by people recording and storing the data, and possibly hosting all such data on their own servers.
220	Indiscriminate collection of data related to individual activity is unconstitutional.

Question 2: Do you have any additional concerns about the use of technology (in case you ran out of space in section one)

ID	Do you have any additional concerns about the use of technology (in case you ran out of space in section one)
1	SPD needs to document the number of vehicles that will have the ALPR expansion. The old SIR and report from OIG states 10 or 11 vehicles but I did not see where SPD acknowledges how many patrol vehicles will have this tech. That's an important feature to communicate to the public.
2	No
3	
4	It will be abused. It is highly invasive and it will hurt Seattle in the long run
5	
6	
7	No
8	Cops have misused this technology in the past. They will do so again. If you give them the ability to track everyone, all the time, they will do it.
9	
10	NA
11	
12	
13	It's perpetuating a gross surveillance state, AS WELL AS being a drain on city funds.
14	
15	
16	
17	
18	
19	
20	
21	Many.
22	
23	
24	No
25	
26	Invasive means. With AI there is no reason the SPD would need to keep this data.
27	I believe that scanning a plate should be up the discretion of officers. Given the circumstances of each individual situation.
28	I agree it’s a great technology and can identify issues very quickly but why does the information need to be saved if no crime? This amount of information saved is a risk to my privacy and recording my location to anybody who requests it.
29	
30	
31	
32	
33	How about also giving an already shameful and abhorrent police force like SPD, who have proven time and again that if unchecked, are capable of depravity equivalent to that of a convicted murderer, access to virtually any american citizen they want.
34	
35	SPD has made it clear that the citizens of Seattle can't trust them. Now they want to track our location in a publicly accessible database. This is insane and I will not vote for any Councillor who supports it.
36	

37	it feels like one of those things that could be scary, but that in order to put it to a scary use a person would have to shift through a mountain of data and know exactly what they're looking for. so, it feels like it's reasonable to require like a warrant or some other reasonable need to access this kind of surveillance, but it's extremely useful and should be used judiciously.
38	
39	n/a
40	
41	
42	Please just don't. Crime is not gonna go down in any meaningful way by this tech.
43	
44	
45	The state wants to surveil the people to control them
46	Also no shot spotter. Technology doesn’t work. Spend money on care for people not hunting them.
47	
48	The police have routinely proven that any power and technology given to them will be abused. Giving them additional surveillance technology will be used to further erode the civil liberties of the citizenry.
49	Divisive political rhetoric not focused on public safety.
50	
51	
52	UW researchers have raised concerns about how ALPR data could be used by federal agencies to track undocumented immigrants or by other states to track those coming to Washington to seek abortions.
53	
54	
55	
56	
57	
58	further increasing our dystopian police state
59	Absolute waste of public funds. It criminalizes all citizens who drive.
60	
61	I am not concerned about non target vehicles being recorded- as long as they are on a public street
62	The rise in cybercrime is also a serious concern in regards to this data, as a bad actor or other state agency could utilize this data with statistical models to track and trace vehicles involved in abortion access, trans healthcare, or protest when or if the Fed ever finds those actions worth suppressing. The FBI and CIA's bad history of assassinating populist leaders outside of the law is also a concern in regards to this technology -- if they can use this data as a portal to track 'dissidents' that will also be a travesty.
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	

73	Our police dept hasn't shown themselves worthy of our trust with data tracking us and, frankly, no gov agency should be allowed to indiscriminately gather such data on their citizens.
74	
75	I believe this additional tech will lead to unethical targeting of low-income, unhoused people and people of color. And it's shown that less than 1% of data captured actually relates to criminal activity.
76	SPD has repeatedly shown contempt for the city it purportedly serves that make it highly un-trustworthy to have access to this kind of technology
77	Images of license plates not linked to any crime should be purged quickly (within 48 hours). This will protect safety of the most vulnerable including victims of intimate partner violence, stalking targets, and others whose safety is not considered when big data sets are put together.
78	The idea that private citizens can access this same data through a public information request is horrifying. This enables stalkers, violent exes, criminal tracking of potential targets, tracking of political opponents. It is ludicrous that SPD is pursuing this when there is such a horrific loophole.
79	
80	As at attorney, I have further concerns about the civil rights of accused people. I work every day with young people who suffer the aftereffects of being stopped by police for being 'in the vicinity' of an alleged crime or somehow 'matching the description' of adults the police are looking for. Often the only resemblance is race - as perceived by officers. My legal work is also focused on domestic violence. The availability of a trove of public records that would allow stalkers and domestic violence perpetrators to track their victims with collected police data is a real risk. This technology is poorly contained, unnecessary, and violates privacy and safety for everyone - but especially for our most vulnerable neighbors. Please reject it.
81	
82	Have they caught the guy who killed Jaahnavi Kandula yet?
83	
84	
85	
86	I am a technologist by trade and I am extremely opposed to the use of surveillance technology.
87	What laws are in place to protect citizens? What accountability is there in place for police officers' misuse of data? What prohibits the selling, sharing, or transferring ALPR data? No way to opt-out.
88	
89	
90	Cost as well
91	
92	That the license plate numbers will be held for 90 days if they do not match up with stollen vehicles. Why so long? We're talking huge numbers of license plates being recorded. Why not work on the system to improve the input of stolen vehicles at that end of the process?
93	This technology puts everyday civilians in harms way and treats everyone as criminals always being under surveillance is a dystopian nightmare
94	I am a technologist by trade and strongly oppose this.
95	The cost? What are the costs? There's not a lot of information on how much it'll cost as a one-time cost and then as a repeating cost. Also, this form was down for over 3+hours, will you extend the commenting period?

96	
97	I am concerned that this technology monitors the public, while studies have shown that only 1-2% of license plates come up as "hot", not enough to store everyone's data for 90 days.
98	
99	This will make things even more dangerous for victims of abuse and dv!!
100	
101	
102	
103	
104	My lingering concern is that the city will fail to use this data to protect walkers, bikers, and transit users from the harm that poor drivers cause. Cars and trucks used in an unsafe manner need to be immediately impounded and the driver surrender their license. Poor drivers must be taken off the streets FAST. Poor drivers need to stop driving and use alternatives such as transit, biking, or walking so they understand how their poor driving affects others.
105	
106	
107	
108	
109	
110	The technology is too invasive toward law abiding citizens
111	
112	
113	
114	Yeah, it's a direct violation of everyone's right to privacy
115	
116	
117	Also, it's scary that a public records request could get this information as well. Not connecting the license plate numbers to the names they're associated with doesn't actually help that much when someone stalking their ex already knows the plate number.
118	Just don't do it. The rate of success from capturing the plates does NOT outweigh the harm that can come from it. The increase in racial, gender, and sexual violence should give you pause as this tech could be used for targeting vulnerable groups and individuals.
119	See a pretty girl driving by? Jot down her license plate and use the database to stalk her digitally, perhaps to her home. (!) We as a society must reduce use of surveillance technology, not expand its use and availability.
120	I lack confidence in assurances this technology expansion will not result in abuse.
121	
122	
123	
124	n/a
125	None
126	
127	Deployment without ethical and privacy considerations that center those furthest from justice.
128	
129	
130	
131	
132	If Cops keep tabs on all citizens plates then aren't we are all criminals in the eyes of police.
133	
134	
135	

136	
137	Expanding police surveillance at a time when public confidence in the SPD is low is personally undesirable
138	
139	
140	
141	
142	Access by the public, and officers for reasons having nothing to do with enforcing laws.
143	Yes! Stalkers can acess this information, which is inherently concerning. Victims of domestic violence are also put at much higher risk because acess to this information is available through the fredom of Information Act.
144	
145	This data will be required to be shared with members of the public who request it. This is tantamount to an invasion of privacy. This data could be used by abusers who want to track their victims of domestic violence.
146	
147	Clearly your transparency is low to middling. Why should we support this being rolled out to the whole force?
148	
149	
150	You could spend the money on schools, parks, and libraries.
151	
152	I don't feel Seattle should become a surveillance city, and SPD fleet-wide deployment would become a literal vehicle for mass surveillance. I should be able to travel through the city without documentation of such.
153	People shouldn't be able to look up plates that cops shouldn't have been collecting anyway. We're layering bad on bad.
154	
155	
156	
157	None right now.
158	
159	
160	
161	
162	Please see #1
163	Yes, it is unethical to follow someone’s every move in their car for 90 days.
164	Yes didn’t run out of space but cannot stress enough that this is not necessary and will do nothing to improve public safety or police and community relationships. There is no reason to further step into police state functions . Currently myself and I think the public do not have enough trust in the police or SPD leadership/ procedures to believe that this will be used wisely or fairly or do anything to actually protect individuals in the community, it extends police jurisdiction, influence, and intercession into private lives. SPD is not in a place to carry out these intents fairly and in a way that supports public safety
165	Information like this can seem simple to discuss in terms of its current known uses, but it’s important to keep in mind that many risks arise from tough to predict queries or inferences made by bad actors with access to the data in aggregate or alongside other information. Decisions to store and make this info available to officers should be made with a longer term point of view in mind, and with the assumption that data breaches are highly likely in the long run.
166	On the whole, I foresee a software that wastes police officers' time on false positives and leads to increasing of police intrusion on folks' lives, with the expense falling on those whose lives are made worse! Why should citizens pay taxes into a software that monitors their everyday actions? It's already a travesty that we're wasting money on Shot Spotter, which is KNOWN to WORSEN outcomes in every city where it was implemented. Why would we want another money pit that makes our lives more surveilled and less safe?
167	This is also a ton of money going to a not proven technology when the city is cutting funding for so many other things. SPD should not be able to hold the data for 3 months either.
168	

169	I believe it is also a violation of our constitutional rights. The fact that a car, where it goes, where the people live, what they do and who sees the information is unconstitutional.
170	yes invasion of privacy
171	
172	
173	Data is open to misuse. SPD has a history of abusing their databases.
174	
175	
176	
177	
178	
179	Why not put this money to expand a murder empire into schools and education if you want to protect the public?
180	
181	
182	There is no good reason why SPD should retain images of license plates that are not associated with crimes for 90 days. These non-hit images should be automatically purged within minutes or hours, as is done within other U.S. jurisdictions using the same technology.
183	The current level of ALDR with its 90 days retention as a public record is already a hazard to all Seattle citizens. The City should first set up appropriate systems and safeguards so that it can handle these data appropriately before seeking to expand the system.
184	
185	
186	
187	
188	
189	I am concerned about the lack of substantial restrictions on how ALPR can be used and how long license plate and vehicle data can be stored in SPD databases. Multiple instances of institutional abuse have occurred and would likely continue, as SPD officers have used ALPR data to track people in their personal lives. Additionally, members of the public can access this information via public information request. The vast majority of this data is on civilians completely unaffiliated with criminal activity, as multiple studies on ALPR have shown that only up to 2% of license plates captured are associated with any crime.
190	
191	
192	Secondly there's been evidence to show that this technology is minimally effective and like any infrastructure it costs money. Installing this system would be frivolous and wasteful for this reason
193	Also, if a person is a suspect and then found not guilty, why should his/her private information be allowed to exisit in a public place that others could use in way to hurt the person. Records should not exist for 90 days.
194	
195	
196	
197	
198	
199	
200	
201	
202	
203	
204	Storage should be limited to 1 day and only for people who have committed crimes
205	

206	
207	
208	
209	
210	
211	It costs money and every dollar not spent on housing and healthcare is the equivalent of paying people to commit crimes
212	
213	
214	This is a privacy issue, an equity issue, and a spending issue.
215	Fuck 12, fuck SPD. Stop the militarization of the police. They are a money suck and a resource vacuum for the city. Defund, disband, and give the money to the community.
216	
217	Do not support the use of this technology.
218	
219	
220	Easy for this information to be misused.

Question 3: What value, if any, do you see in the use of this technology?

ID	What value, if any, do you see in the use of this technology?
1	Seattle's stolen property has been escalating; I see that in SPD's crime reports. Something ought to be done, and ALPRs are potentially a solution. But the database does not add enough value when one considers the potential civil liberties threats.
2	Very little, only like 1 percent of the images captured gets connected to a crime
3	Very little, unless you want to encourage abuse and mistrust.
4	None. 1% potential crime reduction is basically inert. Be better at policing, and investigating not data gathering. Data can be twisted to fit any narrative, good investigative work by definition can't.
5	I get that detecting plates is useful in finding stolen cars rather than manually scanning. I don't think there is any reason to store that data at all.
6	None whatsoever.
7	Stopping gang bangers who did drive-by shootings and home invasions
8	If I wanted to know everywhere anyone uses their car, who they are dating, and where I could go to find them, I'd be able to do this. Is this OK with you? Can we track all city council members too?
9	It will make tracking of wanted vehicles faster and easier. Fleeing suspects would have a harder time eluding enforcement. Parking scofflaws and people with license violations would have a harder time continuing to drive.
10	If the data were not collected and stored, I could see the utility for pinging someone to observe a stolen car or a car mentioned in an amber/silver alert. But as the data is collected and stored, I think any utility is moot.
11	None
12	None
13	I see no value.
14	Absolutely none
15	
16	None.
17	None
18	None

19	Nothing, compared to the already widely utilized instant matching of wanted license plates. Collecting the data for later processing is the same concept as having an officer sit in every citizen's car, just in case they commit a crime. Absurd violation for privacy, isn't it?
20	None, it does not prevent, deter or detect crimes and SPD policy does not permit vehicle pursuits so there will be no effect if they catch someone "in the wild".
21	As currently implemented and given an automated, near immediate purge of records, the technology may be helpful in identifying "hot list" vehicles.
22	
23	None
24	The value is only known after a crime is committed and the need to gather information becomes clear.
25	I have witnessed a large increase in poor driving over the past 2-3 years: speeding, ignoring stop signs and blinking lights, passing in bus lanes and middle turn lanes, and ignoring roundabouts. I'm not going to speculate as to why this happens, but it is putting a lot of people in danger, particularly pedestrians. I think that if drivers were aware that their driving was being monitored, they would drive in safer ways.
26	Frankly, none.
27	
28	It's great when used to catch criminals but why save the data of a law abiding citizen so that people could then request the info and track my locations and patterns.
29	None
30	I'd ing cars matched to crimes.
31	Reduce crime and missing persons. I'm all in
32	None
33	The only value I see is adding one more of our civil liberties taken away from the FREE PEOPLES OF THE UNITED STATES in the name of "protecting and serving". Last time I checked, the police only have a payroll because our taxes pay their salary. They work for us not the other way around!
34	The only point of this technology is to increase the reach of the surveillance state
35	None
36	
37	both times my car was stolen this technology helped find it within a week.
38	I don't. We haven't needed this technology before, we don't need it now, and there is not evidence that it helps police solve crimes.
39	I don't see any value of tracking citizens who are not suspected of committing a crime, who have not committed crimes or are not going to commit crimes. Once again, I see this as a constitutional issue and potentially a crises. What's next?
40	I see value only if the technology is used to be linked to a violent crime. If any other images that are not linked to a violent crime at the time of capture, than they are abusing the right to take these photographs.
41	None!!!
42	I'm not seeing it at all... Certainly not at the expense of privacy.
43	I do not see value in this technology.
44	Automated license plate recognition could potentially be useful in exigent circumstances (Amber/silver alerts, etc) when time is of the essence and a person's life or welfare may be at risk. Access to systems of that nature should be highly restricted and use authorized and overseen by courts.
45	Paranoia
46	None.
47	Well, it could enable stalkers! It will help bring about a facist state in which people in Seattle are unable to move surveilled. But those are not good things.
48	I see no value in giving the police this technology.

	Enhanced public safety. Support law enforcement activities. Potentially reduce vehicle insurance premiums. 49 Apprehend criminals, recover stolen vehicles, support Amber / other alerts, locate drunk/impaired drivers, vehicles involved in road rage, etc Pursue vehicles with no license plates or obscured plates
50	I don't see any value to this.
51	
52	Limited value
53	Alerting to on matches to hot lists has value. It makes it easier for cars that have been reported stolen, reported to have been involved in hit-and-run, or other items to be located
54	It will help reduce crime
55	None.
56	None whatsoever by SPD's own data.
57	Very little except the minority of cases where particular vehicles have a linkage to a person suspected of a violent crime but a very large number of crimes aren't violent.
58	none
59	Fucking none.
60	Negative value. Even if it will help solve a few crimes. The collective bad outweighs any possible good
61	In our current SPD staffing crisis, it is important to use tools that can assist officers. Being able to identify vehicles that are stolen or have been used in a crime will assist officers in making our city safer.
62	If this technology were under the purview of SDOT, and could only be accessed by a formal request process in the case of a crime, then I could get behind it. Making the information largely arcane or obscured so public requests to track individual vehicles aren't a threat to public safety, I could see this tech used to assist with the awful driving habits of Seattle's vehicle owners - people in this city love to speed and to do illegal merges and actions out on the road, and this tech could help with enforcing more traffic laws - I think that needs to be 100% divorced from the police, however.
63	While it can reduce crime, data should only be retained for license plates that are linked to a known issue
64	Tracking criminals more easily
65	None
66	None.
67	None, it's truly Orwellian
68	None. The likelihood of it producing any actionable license plates when the criteria for inclusion is "all cars nearby" is nil.
69	It will be a massive assist in stopping vehicle theft, and other crimes that involve the use of a vehicle.
70	Very little if any.
71	Marginal benefits that might come from recovering stolen property or resolving other criminal activity.
72	literally none lol, this has been shown to be ineffective and the long term data hold is unlikely to do anything helpful.
73	For more quickly playing the license plate state game we used to play on childhood road trips.
74	I do not see any value in collecting this data and storing it and allowing citizens to request this sensitive information.
75	No value, only potential harm by SPD. We need more tech for human services, not policing.
76	none
77	I see some value in this technology for helping locate vehicles associated with amber or silver alerts. But as those situations are emergent and time-bound, retaining the data for 90 days and allowing anyone to request access to anyone else's activities poses a risk for abuse and personal safety concerns.

78	There is a benefit in automatic recognition of license plates, enabling drivers to keep their minds on driving. However, there is NO reason to store plates that are not a hit.
79	
80	None.
81	None. There is no way in which this technology will improve my life.
82	this is valuable technology for building a draconian surveillance state where anyone the police don't like can quickly and easily have their life ruined.
83	I like that if someone is driving a stolen car or has abducted or abused a person, the police can more easily find them out in the world.
84	None
85	
86	I see no positive value in this technology, I think it is extremely harmful to the public.
87	Another lawsuit for Seattle / Washington state taxpayers to fund: https://www.eff.org/press/releases/electronic-frontier-foundation-aclu-win-court-ruling-police-cant-keep-license-plate
88	Absolutely none.
89	None for anyone other than the police, which should not be our primary concern.
90	None
91	None.
92	Some stolen vehicles might be returned sooner, but for this the other end of this process must be speeded up, i.e. when a vehicle is first reported as stolen.
93	None
94	None. This will only allow people who have access to this data to further abuse the system and the people being surveilled
95	None whatsoever. I wish they would dismantle them for the cars that already have implemented them.
96	According to data, < 1% of ALPR reads are connected to actual crime. There is no value in that cost-benefit analysis.
97	I can see the value in that it's helpful to scan license plates in real time, it's the storing of that information for 90 days that's disturbing.
98	None
99	NONE
100	
101	Keeping the eyes of the police officers on the road while driving so they don't kill pedestrians in crosswalks. Oh, wait, nevermind, they do that anyway with no repercussions. So, no value really.
102	None really! We don't need more cameras automatically registering identifiable data about people.
103	None! Why have a record of random plates cop cars are stuck behind in traffic?
104	The true value of ALRP is when it is utilized to track vehicles used in a reckless manner, to include speeding, running red lights, and driving in a manner inconsistent with Vision Zero goals. The key is FAST consequences. Poor driving equals car impounded and drivers license revoked immediately. Driving is a privilege, SPD needs to err on the side of the safety, health, and welfare of the public - not the convenience of the poor drivers. The public does not need to coddle poor drivers, consequences need to be immediate and procedures for re-in-statement of licenses and vehicles need to be thorough, costly, and painfully slow. Poor drivers must plan on using transit/bike/walking for years before re-in-statement.
105	None.
106	None
107	Reduces risk of future crime.
108	There is no value to the public of this use of technology. The invasion of privacy associated is a significant rollback of the rights of Seattlies. It should be outright banned, not expanded.
109	

110	None
111	None
112	None.
113	
114	None! It should be tossed out completely
115	Literally none.
116	
117	If the hotlist is maintained on the vehicle and the plate and geolocation information is not stored, it could be useful for Amber alerts and stolen vehicles, things that the officers in the vehicle would be responding to immediately.
118	Not enough value.
119	Surveillance. In the event someone uses a vehicle to commit a crime, that vehicle could more easily be tracked as it travels around.
120	little
121	I see no value that comes even close to outweighing the costs, both financially and ethically. Washington is already a high recovery state for stolen cars already, and we know that law enforcement have a track record of using this tech improperly.
122	Zero.
123	There is no value in retention of this data or expansion of its use.
124	If used to flag specific plates that are linked to a crime (with probable cause) I see the value in recovering stolen cars and catching dangerous felons.
125	Arresting criminals. Tracking stolen cars. Arresting people who break the law.
126	None.
127	
128	None. I do not care. If cops could do their jobs in 1990 without this technology, they can do it now too.
129	
130	none
131	None.
132	No value except to locate vehicles currently on the road, all data should be often and regularly purged.
133	I don’t see any
134	It may help in occasional cases, but the constant mismanagement and misuse of the SPD means that they need to make significant inroads with the community they inhabit rather than spending taxpayer (or any) money on it.
135	In the narrow case were a license plate is linked to a crime, it could provide additional insights that could help establish the timeline or specifics of a crime.
136	I see that with a reduced police force this would help solve some crimes! Would help with all the stolen cars lately, would help detectives that don't have time to investigate, because they're are too few of them.
137	Very little; I have seen no evidence that this technology would have increased case clearance rates, and as it is not a preventative measure it will not materially increase public safety.
138	None whatsoever
139	
140	it would help identify, capture and prosecute car thieves and other crime perpetrators.
141	None.
142	None.
143	Although there is value in being able to track potential kidnapping victims and stollen cars, etc, the data is kept for 3 months under the proposal and is available to the public. It’s violation of privacy is too great.
144	None
145	The only usefulness for this technology is for red-light enforcement, tracking stolen cars and speeders.
146	i do not see the value and i do not think this technology will improve community safety or well-being at all. i think it will make people less safe.

147	If the car matches a hit list plate, sure great, but keeping the information about non-hit plates for such an extremely long time does not look to be gaining any significant public benefit.
148	Getting criminals who are shooting guns everyday off the streets
149	Significant. Reduced time spent doing manual work which means more time for officers in the community. Better ability to track nuisance perpetrators.
150	None
151	Cars are weapons. If they have the technology to scan plates, they should also be able to scan speed. The police should stop people for speeding
152	I don't feel that the technology's value outweighs the liabilities it poses. There is too short a path to city-wide surveillance and too many opportunities for misuse, either by SPD, or outside influences.
153	None or next to none. Police drive around too much anyway. Get out of your cars and engage with the public.
154	
155	None
156	Sure, it makes it easier for cops to drive safely while also scanning license plates. But why the hell would you store any plates that aren't connected to a crime?
157	I presume it enables quicker flagging of problematic license plates.
158	None
159	I see no value in the technology.
160	
161	None
162	
163	None, this is fucked up.
164	None for the police this is just extra monitoring and surveillance with potentially no public safety outcomes and increased risk for discriminatory stops and police responses
165	I can understand that being able to automatically detect when a plate which is on some list of targets is within view of an officer’s car. That said, I do not understand why that detection couldn’t simply trigger an immediate alert for the officer or the police department more broadly instead of needing to be stored in a historical log.
166	Maybe cops would murder fewer pedestrians with their car and joke about it if they kept their eyes on the road.
167	I do not see any value in this technology
168	Slight value with getting license plates of perpetrators fleeing that may not get caught
169	None. I see it as harmful. There are plenty of other ways to track criminal behavior and the thought this will be expanded and result in harm to everyone.
170	none
171	I do not believe the benefits of using this technology outweigh the great costs and risks to privacy.
172	No value - all downsides
173	It is a complete waste of tax dollars for such a tiny success rate (1%-2%)
174	None.
175	I see no value in the use of this technology.
176	This technology removes a lot of the need for officers to manually scan people and vehicles looking for suspicious actors and playing on the officers biases. The only benefit of this technology is that it allows stolen vehicles to be located faster without officers harassing random civilians, and 'time is of the essence' instances of kidnappings and locating vehicles involved in violent crimes.
177	Great for things like Amber alerts and other BOLO items where immediate response is required.
178	I can see that it will be of great value to the police department in assisting them meeting their quota
179	

180	1. If the scanner is reading plates, the cops can keep eyes on the road, and strike and kill fewer people with their vehicles. 2. If the scanner is reading plates, there is less chance for human error in reading plates and mistaking them for "hot" ids, meaning fewer incidents of innocent folks getting pulled over for no reason.
181	I see no value in expanding this technology to all patrol vehicles
182	This technology can and has been used to solve certain crimes such as kidnapping, etc. But purging non-hit images from storage would not significantly reduce the technology's utility in this regard.
183	If the retained data can be restricted to the less than 1% that is related to criminal offences, it will help prosecute crimes.
184	It provides the punitive justice system greater speed and precision, which is not a particularly worthwhile goal.
185	I perceive the value to be minimal other than making it easier for police to prejudge drivers based on looking up their driving records more automatically and indiscriminately.
186	None.
187	There is no value other than militarization and a step further towards total fascist control of the people. This does not sever the people.
188	none - 0.2 percent of plate scans are linked to criminal activity.
189	ALPR can improve the rate at which police officers can investigate vehicles related to theft, felonies, and missing or wanted persons. It can make this work more efficient, and also be used to verify witness descriptions or identifying features of vehicles involved in these activities.
190	None, this is unacceptable
191	n/a
192	This technology is very useful for mass surveillance and thus controlling population. I think it has little to no value within a democratic and free society.
193	Perhaps in finding missing children
194	Compare current upheaval regarding children and TikTok, this tech is gaming for Law enforcement easy to manipulate and power addictive for police.
195	Absolutely none for public safety. The implementation of it will only deepen the City of Seattle's sense of being a police state.
196	NONE whatsoever.
197	There is no value in this technology. This is an attempt to justify the increase in spending for SPD without producing anything of value for Seattle residents.
198	None that outweigh its inherent damage to privacy.
199	
200	Comparing license plates against a hot list is a legitimate use of this technology.
201	
202	While there is a use for this technology in catching people involved in crime, the studies run on ALPR data show the actual usefulness of this is incredibly low, with some top estimates showing that just 1% of all vehicles scanned by the technology flagging cars with associations to crime.
203	If I had access to this data by public request, I would be able to construct more effective cases against police harrassment and targeting of citizens. It is my hope that I would, through correlation, also be able to infer overprofiled neighborhoods, but this would just be a nice bonus.
204	finding people who have committed crimes
205	I do not see how an expansion of this technology would be worth the cost to implement it (including purchase, installation, training, and data storage).
206	None
207	It doesn’t really seem useful for anything other than harassing people.
208	None
209	Negative value, as in, not positive.
210	I do not see value in the technology. Police having this information makes me feel less safe, not more safe.
211	None

212	Obviously this could be used as evidence, placing a suspect at the scene of a crime.
213	
214	None.
215	Negative value. I believe it will worsen public relations with police, specifically regarding trust and privacy. I absolutely do not want my vehicle being tracked by police if I have done nothing wrong. How does that not constitute an illegal search or seizure????
216	Absolutely NONE.
217	None. And studies show it does not assist police much either. Too expensive for not much benefit.
218	I do not see any value of this technology
219	Helpful so that officers don't have to manually enter plates and compare against a hot list. But I think the data should not be stored.
220	Metadata may reveal police misconduct.

Question 4: Do you have additional comments/questions re what value do you see in this technology?

ID	Do you have additional comments/questions re what value do you see in this technology?
1	If the expansion is going to go through, then at least SPD ought to be transparent about it. If this technology is as great as they claim, they should have no problems showcasing evidence of their successes. That also means being transparent about the use of the database.
2	
3	
4	Why would you even consider allowing this? Maybe if images deleted in 3 minutes like they do in another state. Maybe. Or maybe go read 1984.
5	
6	
7	It will help pull Seattle out of its current shit-hole condition.
8	
9	This should be used to find vehicles and people of interest but not to just vacuum up data on everyone just passing by.
10	NA
11	No, there is no value
12	Is this a surveillance state? Can funds be used to expand staff, outreach, and public safety
13	Only for amber or silver alerts, which would necessitate data to back up.
14	
15	
16	
17	
18	
19	
20	
21	What data exists to demonstrate prior deployments were worthwhile? What percentage of scans were used to prosecute a crime or otherwise serve the public interest? Is the current data robustly audited and if so, what analysis has been done (e.g. is a specific person an outlier who accesses it far more than others?)?
22	

23	
24	
25	I would like to see cameras coupled with cameras
26	There is no value in this given the statistics. It galvanizes the further existence into living in a police state.
27	
28	Why keep all the data? What is the purpose?
29	
30	
31	
32	
33	This will only help police secure more funding while giving a terrible tool to the most depraved of our society.
34	Who on earth thought this was a good idea and have they ever seen even one episode of the Twilight Zone?
35	Unacceptable surveillance
36	Helping track crimnals
37	
38	To reiterate, I don’t.
39	I’d like to have a response from the PD. What is their purpose for introducing this?
40	
41	
42	
43	
44	
45	
46	Put community policing walking neighborhoods. Know us as your friends and families not adversaries.
47	Why are we wasting our time on this? Why aren't the people pushing this on the street dealing with crime?
48	
49	As mentioned so many times in the media and others: abuse, misuse, hacking
50	
51	
52	Who will have oversight on ensuring that the SPD does not abuse this technology when it gets expanded? Will that oversight come from an independent 3rd party? -Because it should, the SPD is not trustworthy
53	
54	It will help reduce crime
55	
56	
57	
58	acab
59	It increases Seattle's budget deficit.
60	
61	I am very glad to see SPD and the City trying new things to supplement the declining police force. And this is not new technology to the City just increasing the use of a technology that has been in use already.
62	
63	
64	Overall I like it and agree with it, I just think you have to have safeguards in place to prevent the abuses from the past mentioned in the media.
65	
66	
67	
68	
69	

70	
71	
72	
73	
74	
75	No more tech for police. Put funds toward human services.
76	Even considering this is a misguided use of city resources
77	Police officers have been known (nationwide and in SPD) to abuse access to databases like this. An expansion of the program must involve oversight, guardrails, and protection of the public.
78	
79	
80	
81	
82	they weren't doing their job before, and your solution is to give them more tools to abuse innocent people. You have failed to lock up the known criminals amongst their ranks.
83	
84	
85	
86	
87	
88	
89	
90	Don't use our tax money to pay for this unconstitutional invasion of privacy.
91	
92	I'm concerned about the amount of surveillance and what other crimes from the police will be used toward the public.
93	Why not just train your officer to be better at there jobs
94	Instead of wasting money on this, fix the potholes in our streets.
95	
96	
97	
98	
99	This will make things even more dangerous for victims of abuse and dv!!
100	
101	
102	
103	
104	Please expand Automatic License Plate Readers (ALPR), to traffic lights and lamp posts. This technology needs to help SPD get poor drivers off the road whether an officer is present or not.
105	
106	
107	Please approve.
108	Ban this technology immediately.
109	
110	Again, no value
111	
112	
113	
114	
115	
116	

117	Why exactly does the SPD need to hold onto this data for 90 days? Other places that do have this technology delete it after a much shorter span of time.
118	
119	How is this database being secured? Will malicious states such as Russia and China use the database to track particular prominent individuals living in Seattle whom they want to meddle with, such as U.S. Congress members? What if someone hacks the database and injects malicious false data that artificially and falsely places a person's vehicle at or near the scene of a crime? What if they hack it to remove legitimate data?
120	
121	I am a person who is part of communities that this tech will disproportionately target and impact. I am appalled that Seattle is trying to expand this already unethical tech. I oppose it and agree with the UW Center for Human Rights, the ACLU, and other community organizations that oppose ALPR.
122	I'm a Security Engineer, there isn't enough space in this form.
123	
124	I'd rather go without the benefits of this technology than give up my privacy.
125	I support this but only if technology is used to make arrests of criminals
126	
127	
128	
129	
130	
131	
132	This scanning of all license plates has little to no value and is an invasion of privacy and has the potential to be widely abused by police.
133	
134	
135	
136	
137	
138	
139	
140	
141	
142	
143	
144	What are the mechanisms in place to ensure this technology is not abused by SPD? What are the mechanisms to ensure the privacy of this data that is being collected.
145	
146	
147	
148	
149	
150	Absolutely none
151	
152	
153	No. This technology should be illegal.
154	
155	
156	
157	None right now.
158	
159	
160	
161	

162	
163	Nope.
164	Same
165	
166	N/A
167	
168	
169	
170	
171	
172	
173	Spend your time and money real police emergencies.
174	
175	
176	
177	
178	
179	please don’t use our tax money for this!!!
180	
181	
182	
183	
184	
185	I would be interested to know about the concrete public safety benefits and see direct weighing of these against the almost inevitable abuse.
186	No value. This technology is an active danger to the community.
187	
188	
189	
190	
191	
192	
193	
194	Was the use and standards for this tech included in the ink freshly drying on the year past due contract? Bet a raindrop 💧 Not.
195	What exactly would this data be retained for? Why would it need to be retained for 90 days, a full quarter of the year? Could that money instead be used to improve road navigation, improve bus service, or housing? (The answer is yes, but where you put this money will tell the community a lot.)
196	
197	
198	
199	
200	Storage of scanned license plates should not be permitted. The only use should be to lookup the plate in already existing hotlists, then the plate number shall be promptly discarded if it doesn’t match.
201	
202	
203	
204	do not store the license plate info for more than one day
205	SPD officers who have this installed in their vehicle should be logged automatically every time they use it, including date, time, vehicle identification, and location. Data on which officers use this, how often, and where should be available to oversight committees and the City Attorney's office.
206	
207	
208	

209	
210	Do not increase the use of this technology.
211	Any accidental benefits of surveillance are outweighed by the fact that the same dollars could be spent on sure fire crime preventers like housing and healthcare
212	
213	
214	
215	When will we have TRUE police accountability? Use this technology on the cops, not on the innocent people of Seattle.
216	
217	
218	
219	
220	

Question 5: What would you want City leadership to consider when making a decision about the use of this technology?

ID	What would you want City leadership to consider when making a decision about the use of this technology?
1	Do the benefits of recovering stolen vehicles match or outweigh the risks associated with misreads or high-risk vehicle stops alongside the privacy concerns with the searchable database? If yes, that cost-benefit analysis should be readily apparent to the public.
2	At least requiring as a part of the expansion that the amount of time the data is kept is limited
3	There is no clear benefit to the public, and massively increased risk of abuse.
4	Their citizens. Police are not and have never been a force for justice. They are just force. Allowing them massive data surveillance is about as terrifying for the public as you can get. Ultimately it will drove privacy minded folks away from our city and state only to help police be more lazy.
5	Consider how badly this could be misused by police abusing their power. Consider how badly this could be misused for an officer to stalk someone.
6	Privacy, security, and rights-based concerns over baseless claims made by a police force that has been a national embarrassment for a decade.
7	Implement it
8	Do not allow this to happen
9	There needs to be controls and oversight of who is allowed to access the data and for what reasons. No officer should be allowed free access to the data. The public should not be allowed access to the data without court allowed access to specific parts. Officers should not be allowed to search outside of cases that they are working on. Officers should be registered and tracked as to which data they access and for what reason.
10	Did drivers in Seattle agree to give up their privacy and control over their data in order to use city streets? Does this surrender of data not usually come with a user agreement, some indication that people know and understand their data is being collected? This technology has already been used in Seattle for a few years now, and I wasn't aware my location data was being collected!
11	The cost of adding this to all patrol vehicles, and the lack of benefit provided. Money could be better spent elsewhere.
12	Weigh the degradation of our privacy and how the technology will/can be abused
13	It's a disgusting use of funds.
14	Start working for the public interest
15	Consider that you might not want to provide an agency that already abuses your constituents with more power and information that can be used in abusive ways. Consider what would truly be gained by this move. Consider what will allow you to sleep at night.
16	Consider the creep in police availability to track individuals who are innocent of crimes. Consider that we are innocent until proven guilty and should have the right to move freely without tracking. How could this be used against POC especially when SPD has historically harassed and arrested marginal groups.
17	

18	Consider what the money spent on this could be used for other, proven programs that actually help people and prevent crime.
19	Although there are many hypothetical scenarios that paint this technology as a silver bullet to save lives, I implore decision-makers to look behind the hypotheticals and question the performance of the currently implemented system through hard numbers today.
20	The current failures, consent decrees and issues that exist within SPD should not give you the rationale or confidence that the SPD will not abuse this technology as they have other items. The potential benefits do not even come close to the risks of the usage of this technology and the city wide implementation of it. Why are they so focused on gathering this information? What use is it? Surveillance of the public at large with no rationale for it is the start of further erosion of civil rights and the allocation of additional power to the SPD that they do not need nor have the proven they have the ethical, moral or human kindness abilities to be entrusted.
21	The Seattle Police Department has demonstrated not mere obstinance but open hostility to both Seattle residents and the rule of law. They violated chemical weapons moratoria handed down by the mayor and council, celebrated killing unarmed nonviolent citizens, incited panic by lying to the public, sprayed council members with chemical irritants, and refused to answer questions regarding abandonment of the precinct. Policies clearly cannot deter them from abuse. Robust automatic purging should be required for any new surveillance deployment.
22	The privacy of its populace, the possibility of their own data being leaked, the prior history of the SPD in failing to safeguard similar information. e.g. this case from 2018 in which an SPD officer stalked his ex girlfriend via a similar database https://www.heraldnet.com/news/investigation-seattle-cop-used-police-database-to-stalk-ex-girlfriend/
23	DO NOT USE
24	Stop assuming that the police will gather information on unfaithful spouses, people going to medical appointments, and other irrelevant stuff. The technology is needed to catch bad people doing bad stuff. If you do not retain ALPR for the 90 day period then you should not bother paying a vendor for the ALPR at all. The ACLU is no longer a relevant organization that protects peoples civil rights. They hate the cops and will do anything within their power to remove any relevant technology that assists them in their job.
25	
26	The invasion of privacy of the people of Seattle & all who visit. It might be better to spend more efforts tracking the explosion of crime that happens on foot here.
27	Consider the consequences of the abuse of such a system. The working poor who drive to work at night or are delivery drivers in high crime areas being tracked and profiled.
28	I would like you to consider how it's fair to track our movements then keep the data fire so long with no cause. The privacy of a law abiding citizen like myself is in danger. Everyday I'm seeing people drive erratically, speeding through the bus lane, passing in the center lane (through intersections) while i sit there following the rules and watch nothing being done. I see dozens of unregistered cars on the road every day. What about insurance, does this system tie in to insurance verification?
29	Maybe for once having a backbone and not cowering to police interests and business interests over the rights of regular people.
30	
31	How can it be used most efficiently
32	Any SPD officers with credible allegations of harassment or domestic violence should be removed before anything like this should be considered.
33	Consider that government was never meant to be able to peer into every aspect of our lives when nobody ever asked for big brother looking up everyone's skirt without even asking us out to dinner first.
34	Consider literally anything else
35	This should be illegal.
36	What will help the police make our city crime free.
37	it's this, or make it safe to park your car on surface streets in Ballard. (right?? fucking Ballard, they stole my car in BALLARD)
38	That this technology is unnecessary, costly, and dangerously intrusive.
39	Consider a citizens constitutional rights. Otherwise, this will get bigger than the counsel.

40	If City leadership would feel comfortable with all of their movements being tracked, and potentially compiled.
41	Consider eliminating use of this technology by police instead of expanding it.
42	Please do not use this tech against us - Police have proved time and again that they need to earn our trust - this is not a step in that direction.
43	Seattle should not be a surveillance state. This is the garbage that countries like China do invade into people's personal lives.
44	License plates exist as a public safety mechanism for law enforcement and other authorized parties to verify ownership and registration of vehicles and enforce road safety laws and regulations. They are not and were never intended to be a mass surveillance tool.
45	The rights of private citizens
46	False information. Terrorizing citizens.
47	That SPD lied to us about the East Precinct.
48	Consider the public's rights to privacy and their safety from the police.
49	City leadership is ineffective and not the appropriate decision maker. This effort must be lead by law enforcement, along with an politically independent organization, to evaluate data associated with the use and misuse of this technology, address concerns, implement guardrails, then implement state-wide with the ability to communicate between state law enforcement agencies.
50	If SPD is insisting this technology is crucial for doing their job (which I'm dubious about), then please require them to clear all "non-hit" data after 1 hour -- as many other cities who use this technology do.
51	Don't do it. Don't waste the money.
52	The untrustworthiness of the SPD
53	What is the case for expanding the use of this technology? The rate of stolen cars getting recovered is already extremely high.
54	Put it in every patrol car and at fixed locations all over the city.
55	Why consider it at all?
56	Consider the 99%+ of city residents who are not involved in an investigation and may be tracked by anyone who queries the database of retained license plates. There are innumerable ways for this to be misused and almost no utility by SPD's own data.
57	We should also consider the costs. SPD's clearance record is abysmal and it's probably not because they lack this particular technology given that most crimes are never associated with a particular vehicle with a known license plate.
58	acab
59	The potential for city government creating a right wing police state and future lawsuits.
60	Whether they want any member of the the public to be able to track their comings and goings on a continual basis
61	It is important to look at the possible repercussions and weigh that against the public good. In this case the benefit to the public far outweighs potential harm.
62	The above, and that turning our city into a surveillance machine under the purview of police officers with an awful track record is just blatantly a bad idea. If one of the members of city leadership had a falling out with a cop or pushed policy that was anti-police expansion, would they really want 3 months of tracked license plate data at those cops fingertips? I would hope they can see the risk involved through this anecdote.
63	Value citizens privacy
64	Crime and the perception of crime is up and is bad for the city.
65	Privacy
66	Consider residents' privacy.
67	That it is unconstitutional
68	How many women die from domestic violence annually. This publicly available information will escalate cases from mere harassment when abusers only have contact info, to assault and death when abusers can learn where their victims are physically located as part of their daily life habits. Most people go to the same locations for work, worship and basic errands.
69	Beyond having it on police vehicles, maybe have cameras set in high traffic areas or areas of concern to ping when known plates show up in the area.
70	If you do approve this technology, please push back on department leadership who say that 90 days is an appropriate retention period for this type of data. If it is collected, it should absolutely not be stored for that long.

71	1. Whether the marginal benefits of this technology outweigh severe privacy infringements and potential for misuse. 2. Time period allowed for retention of this information. 3. Limiting the scope of which department vehicles can use this information, if any. 4. Who can access this information. 5. Recordkeeping of access logs showing who within the police department is accessing this information and when.
72	The rights of the citizens, the real consequences of this technology, our right to privacy, the expansion of the surveillance state, the ways this people vulnerable to abuse, stalking, and other crimes by allowing personal data to be shared to literally anyone.
73	Other jurisdictions strict standards for data retention and to make sure there are publicly visible checks/balances/reports for those who want to access the data.
74	I want the city to see how spending public dollars on things like this for police is a huge waste of resources that could be spend solving root issues. Also, I want the city to value citizen privacy and security. The police already have enough ability to surveil and track citizens.
75	Please consider the likely harm by police and further distrust of SPD by the public.
76	The impact to communities that are already over-policed
77	Studies of ALPR data show just 1% to 2% of license plates captured are either on a hot list or associated with any crime at all. Therefore, there is not a strong data case to be made for expansion of the program without a firm framework for public safety, limiting how data is accessed and shared, and reasonable data retention limits.
78	Consider in particular the use of this technology in elections. With only a license plate number, any political opponent would be able to track your movements across a 3 month period. Consider also that this dramatically expands the already considerable political power of the police and police officers guild.
79	Please read what I said in question 1.
80	The police department spends a tiny fraction of its time investigating major crimes. They will not do more just because they have more surveillance - this surveillance information will be misused, and it isn't worth the cost, the harm, or the injustice it will inevitably spawn.
81	Why does the police budget need to be so gigantic?
82	Have the police demonstrated quite clearly that they consider themselves to be above the law. They have also demonstrated clearly that they do not have any interest in reducing crime or even lifting a finger to do anything to help the victims of crime, for example by recovering stolen goods. This behavior has been rewarded with constant budget increases and now an expanded surveillance state.
83	Consider all the abuse vectors for people with access to this technology, whether through internal access or the freedom of information act. Consider immediately and automatically discarding any data not known to be associated with crimes. Even if that makes it slightly worse at detecting crimes that the police become aware of after the detection has happened, it makes it a lot more immune to abuse.
84	Look at their past behavior and whether they seem to show respect for the civil liberties of Seattle citizens.
85	Consider the impact on privacy and the way that other jurisdictions manage this data. Cars not involved in a crime should have the data either not captured at all or purged quickly from the system.
86	
87	
88	Think about how easy it would be for anyone to simply request that data and have a map of your movements. If you don’t want that personally, then you have no business deciding that for anyone else.
89	
90	Privacy, violation of the Constitution, misuse by police.
91	The city leadership should bane the technology.
92	Privacy. Ethical problems (already exhibited and hard to stop). Who has access and how it can be used to harm. It says it would be public information, hackers will use this! Scammers will use this!
93	To not force your citizens into suck a predicament
94	Consider how this money could be used to help the community at large instead of using this for surveillance of citizens which leads to abuse of power.
95	People's comments, thoughts, and warnings.
96	The police department is meant to be a public service. SPD has shown again and again that they have no interest in serving the public. City leadership MUST hold them to task. Consider putting funds toward community services that are proven to reduce crime, rather than reckless technology that gives SPD further opportunity to deprive citizens of basic rights.

97	Do not store the data, the technology can be programmed to delete the data quickly.
98	Do not implement this technology.
99	This will make things even more dangerous for victims of abuse and dv!!
100	
101	If City decides the apparent benefits outweigh the massive, consistent invasion of privacy of every Seattle driver, they should at least limit the data retention period to 48 hours or less. If SPD cannot make use of the data in that amount of time, maybe they can spend less time harassing and killing innocent civilians.
102	Please look into existing complaints to OPA regarding misuse of this and related technology by SPD as well as cases of misuse nationwide. Please consider how this technology might be misused to directly put people in danger.
103	Think about doxing and how public info gets misused! It seems like a bad idea.
104	Safety, health, and welfare of the public. City leadership needs to hold paramount the safety, health, and welfare of the public. Every poor vehicle driver needs to be taken out of the drivers seat and use transit/bike/walk. Poor drivers need to understand how their actions impact others. City leaders need to refrain from coddling poor drivers.
105	Stop throwing money at the SPD.
106	The policing alternative this money could pay for instead of police state tech toys.
107	Approve for increased safety.
108	Citizen privacy, SPD's heinous record of corruption, decrease in trust of law enforcement.
109	Erase it within 48 hours unless linked to an ongoing investigation
110	Privacy rights, budgetary costs, less invasive alternatives
111	Technology is not neutral. It can and has been used inappropriately. Once it is in place and precedent is set, harm has been enabled, and it is very difficult to undo.
112	
113	Pray to a loving caring wise humorous beautiful joyous higher power for guidance in this decision. Your soul is at stake. Stay awake!
114	I would want them to simply not consider it at all
115	Do. Not. Do. This.
116	Consider how a malicious actor (within or without the SPD) might be able to track and follow an individual without their knowledge. Now consider how many thousands of individuals could be tracked in the same way with no tangible benefit.
117	Also, how expensive is this going to be? The city has a massive budget problem right now; how is equipping the SPD with more expensive technology going to help this? They just got the "ShotSpotter" thing for 1.5 million dollars. Maybe use that new toy for a while first?
118	Costs, Resources, Success Rates, Personal Privacy and Human Rights
119	All of the above. There have been at least three reported incidents of police using this database for personal purposes. Any vehicle data collected on innocent civilians who are not involved in any criminal activity should not be recorded or stored.
120	unless the data retention time can be dramatically reduced from 90 days (less than 24 hours?), the technology should not be expanded to every police vehicle
121	I want them to consider NOT expanding this technology and to do away with it entirely.
122	Not Doing It At All.
123	Would a City employee consent to having their vehicle's whereabouts tracked, by any member of the public, with no opportunity to opt out? Would a police officer be in favor of any person being able to track their personal vehicle use? If not, this program should not be expanded and should, instead, be curtailed.
124	Please approve this request ONLY if paired with legally binding requirements that prevent the creation of a surveillance database. And include an audit by a third party to verify our privacy.
125	How many arrests can they make and will they actually get criminals off the streets.
126	The waste of money from a cost effective standpoint. The departments are already throwing money away on other pieces of technology, like the shot spotter and the lawsuits from officers abusing their power. The safety of largely women is also heightened when their movements can be tracked by abusive partners and other people in their lives.

127	Is this the right “solution” to your defined problem? What does precedent tell you about the misuse of this kind of collected data? About breaches?
128	
129	Reach of current SPD ALPR devices is already very broad. During 1 week in 2021, 9 active SPD ALPR devices logged nearly 100,000 reads, including outside Seattle city limits, according to analysis by University of Washington Center for Human Rights researchers: https://uwchr.github.io/spd-alpr/
130	stop wasting money on surveillance tech
131	Please be mindful of the rapid pace of AI and how unreliable it is.
132	Curtail this data use to be purged within 48 hours or less.
133	The disproportionate effect that incarceration has on vulnerable communities
134	Fund other things like social services to make our streets and communities safer! Like the library, parks department or DESC!
135	This is not a hard technology problem. If the SPD cannot provide the same guarantees and timeframes that other jurisdictions can provide, that's not an excuse to approve this request. Rather, it's further evidence that the SPD's data control and management systems as so antiquated as to be evidence that abusing this data isn't a risk--it's a guarantee and only a matter of time.
136	I would like them to consider that crime in our city is constantly going up, we don't have enough police officers on the force, and can't hire/train them fast enough. I think if this would help take folks committing crimes off the public streets, I'm for it.
137	Do not underestimate the risk of leaks or improper access; computer systems are not impregnable.
138	Do not use it at all
139	
140	The citizens (disproportionally black and brown) victimized by ongoing crime.
141	This does not prevent crime in any way. Transfer the money to community initiatives to house and feed our cities most vulnerable, which has been shown to prevent crime.
142	Consider eliminating this altogether.
143	Do not adopt a policy that violate people’s right to privacy as provided under the US Constitution.
144	Please consider all the better uses for this money, investments in the community that would actually increase public safety.
145	I request that the City reject the expansion of the use of this technology.
146	please listen to community. we care about our own safety and this will NOT help.
147	The City leadership should take privacy concerns extremely seriously.
148	How many criminals can you lock up?
149	
150	Don't buy it. Invest in the community instead.
151	If the City is going to install technology to can plates, they must also scan speed and stop people who are going more then 5 over the 25mph speed limit. Cars are killing people walking.
152	SPD has other emergent issues at the present time, and new technology, procedures, staffing and other intangibles should not be introduced that could create further issues within the department.
153	Do we really want to give SPD more toys or more power? Police solutions are rarely good solutions. Decrease the police budget, increase social services. It's that simple.
154	Privacy/bias/database abuse
155	
156	Personal privacy, and the ease with which the technology can be used by abusers.
157	I would want leadership to examine carefully whether capturing reams of potentially private data is worth the benefit, and to provide strict, enforceable guard rails to prevent data dissemination. I would like data to be held as briefly as possible, if at all.
158	Who this will affect and how it empowers police to continue abusing its power
159	Is this technology addressing the root causes of harm in our community (housing unaffordability and insecurity, redlining and disinvestment in neighborhoods on the basis of race, lack of health and income supports)? Are there ways to improve health and reduce harm that do not rely on surveillance and policing that the city could fund instead?

160	Please consider our human, and humane, rights of privacy.
161	The impacts of who had access to this data and the many ways it can be misused
162	Please see #1
163	Please consider the privacy and autonomy of the citizens of this city. This type of policing is not ok.
164	Openly asking community members and giving information sessions, looking for real ways to connect with the community to increase public safety instead of trying to sneakily monitor people; pick better officers who are willing to work with people where they are and able to listen and work in a harm reduction model instead of an escalation and surveillance model, go out in the community and actually connect with people and do active patrols to be visible; ask SPD leadership at the precincts to instruct their staff to respond to calls and actually connect with the community and listen to their needs - currently response times are terrible, there is already a staffing crisis In SPD, and much too often there is no actual response for many hours because it seems that officers refuse to leave the precinct. Better accountability measures for officers that are not punishment based and look to train and correct behaviors to improve police community relations. There are many more important and needed things SPD can and should do to serve the community expanding monitoring, or teams like CRG that have no real value to the community does nothing to address the goals SPD outlined for this proposal , bring back community police teams localized in each neighborhood
165	As suggested above, I would strongly urge city leaders to consider that the use of this technology cannot be promised or predicted upfront. Once the information is available to police, new uses or abuses will be discovered and leveraged.
166	There is a very real danger to victims of abuse and stalking in keeping a registry of license plate locations. This danger only increases when you realize how commonly police are those perpetrators of abuse. Further, this technology undermines basic privacy and the ability of people to feel safe going about their lives. I, personally, would not feel safe visiting local queer support centers if I knew the government is building a profile about where I go. I can only imagine how much terrifying it is for others-- those who would not want to be on a registry for visiting abortion-giving clinics, or places of worship.
167	Leadership should think about the harm this can cause individuals going about their daily lives in Seattle. Especially those experienced domestic violence where people can look them up with a public records request. And with the disproportionate domestic violence perpetrated by police officers, this is also cause for concern with their access to this. Beyond this, increasing this technology will be hugely expensive and the city has more important things to fund that actually meet people's needs.
168	Purge the data much quicker than 90 days. 1 day is sufficient. Plus housing all that data is going to be expensive for 90 days.
169	The City Council and Mayor needs to consider their constituents privacy and the fact that the technology will also cause harm to innocent people
170	
171	I want City leadership to, at minimum, avoid technologies that would enable routine surveillance of individuals not under investigation/not under a warrant. This is a huge overstep.
172	Consider voting against this and all other surveillance technologies in public spaces funded by taxes, which includes roadways.
173	Find a better use of our hard earned tax dollars.
174	Civilian oversight into how civilian data are stored, protected, accessed, and expeditiously purged.
175	Consider how increasing the surveillance on citizens and the tracking of their movement limits their rights to privacy, and the INCREDIBLE number of ways this technology can be abused. Given the inefficacy of police in preventing or helping resolve any crime, why would additional technology to help them track and surveil more be beneficial to the public?
176	This technology is unnecessary, if you must expand money we spend on policing, an already bloated area of the city budget that sees zero returns on investment for public health and safety, please ensure that restriction is placed on the data this technology creates to limit unnecessary tracking of civilians. There are consequences to using this technology, expanding the constant surveillance and tracking innocent people throughout their lives with zero technological mitigations on that surveillance is an unacceptable consequence that should deter the technology from being used at all. We cannot create a jail cell for every citizen to live in just so that we may not worry about 'crime', consider the humanity of everyone in the City and the desire of every human being for freedom from being constantly watched. Do NOT allow data from non-hits be kept for any longer than an hour, there is no excuse, the department cannot be so inept that it cannot identify a "significant image" within that time-frame.

177	Recognize the opportunities for abuse of this data and put controls in place to ensure that it is not abused. The existing ALPR data has already been abused by SPD officers for harassing ex-lovers and ex-lovers new relationships. This is unacceptable and there must be guardrails against this kind of abuse.
178	I would like them to consider who will benefit from increased surveillance.
179	
180	Like all data-gathering technology, it's very useful and also very easy to misuse. Any expansion of the use of this technology MUST be accompanied by an extensive set of guardrails around its use: how long is the data available; who can access it; when can they access it; what kind of evidence request do they have to make to access it.
181	Digital privacy rights being violated by the blanket use of this tech
182	A thorough risk-benefit analysis must be done for such a sweeping change. The expansion of this techology cannot be approved until strict and mandatory audits and regulations are in place. Require that SPD explain in great detail why non-hit license plate images must be kept for months, while other jurisdictions purge them almost immediately. SPD should be made to PROVE that the benefits outweigh the risks - it cannot be assumed. SPD has already proven that even officers within their own ranks have used this technology improperly and for criminal stalking. Thus, they cannot be trusted to make promises about the utility of this technology without data to back them up.
183	The City should first set up appropriate systems and safeguards so that it can handle these data appropriately before seeking to expand the system. To do this the City first needs to learn from other states like NH and set up a system that can quickly identify data relevant to crimes and purge the rest. There should be an additional safeguard that the data of any innocent citizens should not become a public record.
184	Rather than funding efforts to 'catch more criminals' at the cost of 'pesky civil liberty' please try to focus on changes worthy of upholding.
185	Put a premium on privacy, and let the data lead us to the most effective tools. Generally solid investigations and building trust and relationships in communities. That starts with addressing the culture problems in our police force.
186	Does it feel "safer" having your personal information secretly scanned without your knowledge and put into a police/publicly available database when you were going to the grocery store or on the way to your house or just passing through? No, this does not improve public safety.
187	Consider how data is weaponized in our modern world.
188	The council rejected amendments to add money to our city foodbanks this year. Income disparity and food insecurity are major problems the city is facing - and even a small amount of money can make a huge difference when it comes to food security. Spending money surveilling Seattle citizens should not be council's priority.
189	These steps toward techno-solutionism in our public institutions cannot be taken without the expressed consent and overwhelming support of the people whose data, privacy, and lives are at risk. The constant pushing of the needle towards increased 0collection and maintenance of detailed information about multiple aspects of our lives as the price to pay for participation in public spaces has already gone too far, and this will only take us further in the direction of fear, surveillance, and corruption.
190	This will not help prevent any violent crime but will be used by nefarious users to stalk intimidate and harass constituents
191	Please consider the safety of people experiencing domestic violence, people trying to escape trafficking, people seeking access to services such as abortions, and people who are being stalked, to name just a few situations in which access to tracking information could pose severe-- even deadly-- risk to the people in them. This includes civilians who have no personal relationships to SPD officers, but who may have people in their lives who would use access to this information to hurt them, and it also absolutely includes people who have personal relationships to SPD officers-- multiple SPD officers have already used ALPR technology to stalk people in their personal lives and NO ONE (SPD or civilian) should be able to access such sensitive information.
192	Is sacrificing the freedoms of privacy and laying the ground work for mass surveillance of the public worth a possible small change in road crime?
193	Look at other states that quickly discard the surveillance infomation..
194	As we are paying for the love of tech and damning efficacy, community involvement in implementing and a MOU of this surveillance program and local tech TB purchased/ considered from local vendor. Lastly no bevy of paid consultants to monitor, disseminate or staff this misadventure.

195	A large majority of the non-white community in Seattle already has difficulty trusting the city council, and even less so the SPD, which again, has repeatedly shown bias against particularly Black, Native, and Hispanic communities for several decades. Adding a way to track vehicles is dystopian and would erode that trust further.
196	Consider the killing of Manuel Ellis. Consider all the misuses of power of SPD. Consider their handling of the 2020 protests. Consider the ways that police have tracked and killed activists, innocent women, and even just those they have political or personal grudges against. Consider all the fucking ways this technology could be abused and for so little potential value.
197	City leadership should consider the wants of the residents of Seattle. This level of surveillance, available to both SPD and the general public, is outrageous and dangerous. This is again an attempt to justify the increase in spending for SPD without producing anything of value for Seattle residents.
198	The use of this technology should be not be expanded, rather it should be curtailed or eliminated. The system should not retain any data related to non-hits for a period longer than three minutes. If the system can't meet this requirement it should be scrapped, and only replaced by one that can and does.
199	The certain impact on people's privacy. The liability of having to safeguard this information once collected. The potential damages the public can claim if this information is abused or exposed to adversaries.
200	
201	Consider the costs - both financial and erosion of civil liberties - that expanding this camera program represents. SPD shouldn't be wasting their time and resources with a system that can't automate looking through massive numbers of images and being able to quickly determine whether they need to be retained our not. It is unacceptable that these images be kept for up to 90 days and that they can be accessed both by law enforcement and members of the public via public disclosure.
202	Have the database that people's identification information stored in emptied much more often than the current 90 day mark. SPD stores this information for already much longer than many other departments around the country. Record who has access to the database. If the OIG doesn't know which officers can access this database and there are reports showing that current police officers have accessed information on an ex's new partner, or information on a domestic violence situation and then revealed that to a party involved, there needs to be a way to hold those people accountable. That this is not already a policy or practice is irresponsible and shocking.
203	
204	Privacy laws and the collection of data about citizens who have not committed any crimes
205	SPD's case closure rate has continued to decline despite increases in budget and new technologies. This is a waste of money that could be put towards solving root causes of crime, rather than give SPD officers a way to track any citizen they please.
206	Consider that this is taking rights away from good hard-working Americans Freedom that we are entitled to privacy is being stripped from us and this is absolute violation
207	The fact that police always lie and are never held accountable. Providing them yet another source of data to surveil the population for no gain should not fly.
208	Putting the privacy of people over what SPD wants for surveilling people
209	Don't adopt it
210	
211	That we don’t want more money going toward police or policing
212	This is police overreach that invades people's privacy.
213	To not do it
214	SPD do not need more technology with which to further abuse our trust. This is a notoriously corrupt police force. OPA has received an average of 1,200 allegations of police misconduct over the last few years. There are numerous examples of SPD inappropriately accessing data: for example, in 2021, a police officer used his access to databases to track his ex's new boyfriend. Now they want more surveillance tools?

215	the fact that this will very likely reduce the public's trust in police and I am very certain that bad actors, in SPD, city government, and private individuals will use this info to harass people they don't like or have political differences with. Think about how this could affect folks escaping DV, to have this information publicly available could put them in harms way. 40% of law enforcement spouses report DV. Keep that in mind…
216	Do not further entrench your constituents in a hostile surveillance state.
217	To not move forward and spend the $$ elsewhere.
218	Consider alternatives that give to our community rather than increasing surveillance.
219	Consider the ease with which members of the public will be able to download the data and keep it forever.
220	Think on compromising your privacy.

Question 6: Do you have additional comments/considerations that leadership should take into account when making a decision about this technology?

ID	Do you have additional comments/considerations that leadership should take into account when making a decision about this technology?
1	Republican attorneys general have been seeking methods to extract information about their residents fleeing red states to blue states seeking reproductive or gender affirming care. City leadership should find a way to prevent this technology - especially the database - from helping to prosecute individuals who lawfully enter Washington state for these healthcare needs.
2	
3	
4	Shouldn't police do police work? Maybe have better ways to police than mass surveillance.
5	
6	
7	Implement it yesterday
8	
9	
10	NA
11	
12	
13	
14	
15	
16	Absolutely do not do this.
17	
18	
19	
20	Trust is earned, not given and the SPD have not earned the trust needed for this type of request. They need to work through the existing problems and remediate them before they can be given any additional abilities.
21	The City spent approximately one third of its total budget on SPD. It's well beyond time to stop throwing money away by buying them every shiny toy they want.
22	
23	Don't expand this don't use it
24	No
25	
26	Please show respect for the obvious, blatant, invasion of privacy of this is & ultimately how innocent people may be victims of this data.
27	The SPD has abused this system in the past. The ALPR system will allow for abuse of power that is arguably goes against the 4th Amendment of US Constitution.

28	
29	This is all so creepy. How are you even having this conversation?!
30	
31	No
32	SPD continues to employ officers convicted of crimes and who have committed gross misconduct. Until we can get to a point where SPD is not employing individuals who have demonstrated a lack of willingness to comply with the law and SPD policy, leadership should not allow the authorization of any technologies that could be abused. The department also needs to implement better systems to prevent technology it already uses from continuing to be abused.
33	Stop this insanity. Only you can prevent forest fires.
34	This is a terrible idea
35	
36	
37	
38	Seattle has been a leader of police reform since 2020. There is no need to expand police powers and set back years of work.
39	Don’t vote for it. Otherwise, this will be a stain on your record.
40	
41	
42	
43	
44	
45	You don't rule us
46	Technology is a cheap choice. Not in terms of money but in terms of care for our community. Not everything can be fixed with tech regardless of who’s selling it.
47	
48	
49	Communicate with insurance providers to seek input, and possible technology funding, relative on the tangential benefit to that industry.
50	
51	
52	The untrustworthiness of the SPD
53	
54	
55	
56	
57	
58	acab
59	Do you want your private vehicle and personal location tracked by police?
60	Please oppose any measures that increase broad spectrum surveillance.
61	
62	
63	
64	Enforcing rules is how you maintain a civic society
65	
66	
67	Don't do it.
68	With budget cuts looming and the police already having a disproportionate amount of that budget, this is a poor use of that money. The citizens of Seattle marched for George Floyd for days to protect against police overreach. This would give cops more power in direct opposition to the will of the average Seattlite.
69	
70	
71	
72	why does SPD need 90 days of data when plenty of other jurisdictions delete this data so quickly?? does SPD just suck at their job?

73	
74	
75	No to this and no to shot spotter.
76	
77	
78	Consider also the security and cost of storing this data. Data storage isn't free and the security is never perfect. What are the infrastructure costs of storing this much data (again, data that has no investigative benefit and a massive amount of liability)? What would the fallout be if this system were hacked or the data leaked? Data in storage is vulnerable data. The longer data is held in storage the longer it is vulnerable.
79	Please read all of the text that I submitted in question 1.
80	
81	Police have always used their tools to oppress people and engage in campaigns of systematic harassment of anyone who criticizes them.
82	I know it is hard for you, but please consider that the police are over-funded and the rest of the city is woefully under-funded.
83	
84	
85	We should be concerned NOT ONLY with how the police could use this data (which should be a concern), but also with how the public can use this data.
86	
87	
88	
89	
90	Cops and the mayor love new, untested, expensive cop toys like the shotspotter and this proposed garbage. Stop it!
91	The city leadership should listen to the will of the people, or be ousted from government by them.
92	Yes, we don't know who will have access to this data and what harm it can do. Not every police officer is trustworthy with such information. There are already proven abuses from this kind of close information.
93	To listen to the community
94	I will be actively campaigning against this
95	yes, have they done any research themselves on ALPR?
96	
97	
98	
99	This will make things even more dangerous for victims of abuse and dv!!
100	
101	
102	
103	
104	Expand ALPR. Red lights. Speeding. It is within the city's power to make our city safe for everyone, to attain vision zero goals if leaders expand this technology to "drive" every poor driver from the streets of Seattle.
105	
106	
107	
108	
109	
110	Stop spying on people!
111	
112	
113	
114	
115	How are you going to ensure this will not be used to discriminate against marginalized folks? Especially when it’s in the hands of SPD who have a LONG history of discrimination.
116	

117	
118	Read the reports. Review the literature. Know the facts.
119	Will there be a means for vehicle drivers and owners to opt out of this database? What is the argument for making this database publicly available to the public and worldwide (assuming it is made available on the Internet), versus keeping it for use only by law enforcement? What safety measures are in place to ensure law enforcement personnel or would-be abusers are using this database in a sanctioned manner, with permanent logging of all usage? Will all use of the database be recorded, such that if someone is raped, attacked, killed, etc., by a criminal who used the database to locate their target, then the criminal's IP address and own database usage can be used to identify and locate them?
120	public confidence in our police force is the issue
121	From an equity and a human rights standpoint, ALPR is a bad direction for our city to move in and does not add the value that proponents argue for.
122	"Law Enforcement" has a tendency to you know ask for things that are Against the best interest of citizens while talking about homicides, robbery, kidnapping and pearl clutching about The Children. This is precicely the same formula.
123	
124	I support our police having tools to do their jobs. But only with well defined limits and third party audits. This technology comes with significant risks to the public good. Let's do it right. Flagging known plates is fine. Mass data collection is not.
125	No
126	Stop wasting money and focus on fixing your culture and training. No one can trust you when you have so many bad actors.
127	
128	
129	Under current data retention and public records policies, anyone could obtain up to 90 days of SPD's ALPR records and track the movements of specific license plates throughout the region. This presents significant privacy concerns.
130	
131	
132	Seattle barely is starting to trust cops again, this will not improve the situation
133	
134	Please stop this incessant need to spy on the community and instead look to invest into it!
135	
136	Think more about the lives this will save or crimes this will help solve, more than if we should use it. If we use it responsively it is well worth the additional cost.
137	
138	
139	
140	
141	
142	Require deletion of non-matched data as soon as the matching process is complete.
143	
144	
145	
146	
147	
148	
149	
150	This technology will hurt not heal our communities.
151	
152	
153	Police don't need more tech. If anything, they should be on foot more making face to face interactions with people. We don't trust the police because they're an occupying force. We don't know them. They aren't from our neighborhoods.
154	

155	
156	Same.
157	None right now.
158	No
159	
160	
161	
162	For any retained data, assume that it can be obtained by those who will do the worst things with it. Facebook and google data provide great examples of how states with agendas can extract information via court requests and do things with that data that impact human rights.
163	
164	Try harder, instead of looking for the easiest route look internally to assess training and corrective procedures so that staff are better equipped to handle complicated calls. Connect with the community and be open about intent instead of trying to sneak in extra surveillance measures
165	
166	
167	
168	Consider budgetary overruns and impact for privacy.
169	
170	
171	Leadership should consider not just intended uses of data but also the potential for abuse and harm that exist if the data is not used as intended.
172	Overreach of power - capacity to track movements and retain info on people - high cost of this technology when there are other pressing needs/ social services that should be funded - the potential for abuse of this data by police - the potential for abuse of this data by other than police - I oppose increasing surveillance of people going about their day-to-day lives.
173	Listen to the public. Many of your policies fly in the face of the public good.
174	
175	
176	
177	
178	
179	
180	Is the benefit to the police department large enough to offset the cost to our privacy. Is the police department prepared to respond to the spike in DV calls when abusers have accessed their exes' travel logs using FOIA resources. Is the police department actually able to disregard looking at the patterns in traffic around big planned protests in order to protect the Constitutional right to privacy of citizens, or will they insist that reviewing that data is necessary for public safety.
181	
182	Any proposal that includes sharing data with other states or agencies outside of Seattle should be a non-starter. Any proposal to store non-hit images for 90 days should be a dealbreaker in terms of expanding this technology.
183	
184	
185	
186	The city desperately needs more extreme weather shelters for both increasingly cold winters and consistently smoke-ridden summers for the homeless population as well as people whose houses are not equipped for extreme weather. Extreme weather shelter expansion would be a much better use of these city funds and improve public safety far more than expanding automatic surveillance technologies which will actually diminish public safety.
187	
188	Please consider this technologies efficacy. If the technology were able to solve crime it would be worth while to consider. But given that 0.2 percent of plate scans are linked to criminal activity and the number of concerns this tech brings and potential abuses, please weigh carefully benefits and risk as well as consider how this $ could be better spent. If we are concerned about car theft - our tax payor dollars would be much better spent on lighting and environmental improvements that have been shown to reduce crime. This would produce a

	greater benefit to the public in terms of public safety without any concerns for the privacy of law-abiding citizens.
189	
190	Those in witness protection or in refugee status or otherwise at risk of stalking or surveillance should not be able to be documented at locations that are then accessible through FOIA, public records requests and through as large of a network as the Spd
191	
192	see Edward Snowden
193	
194	See above
195	You have the power to make this community better and safer; allowing a uniformed police force to track cars at their own discretion leaves an unacceptable risk of targeting non-white communities. Please consider spending whatever funding this takes on something that tangibly helps the community at large.
196	
197	
198	When this information is collected it becomes subject to abuse by both authorized and unauthorized parties. We cannot effectively prevent this access, or abuse, therefore we should not collect the data.
199	
200	SPD has not demonstrated it's a good steward of license plate data, so it should not be permitted to retain data. Other police departments accomplish their goals without the need to retain this data, so SPD should be able to operate without retaining license plate data.
201	
202	Is the technology actually useful? Technology like this is always touted as something amazing that will revolutionize some part of something, but not only is it expensive, it's benefits are always way overstated. Is the expansion of the program really necessary? Or is it just something that a department wants to do?
203	
204	Protect privacy
205	
206	
207	
208	
209	
210	
211	Defund SPD and expand housing as fast as possible
212	
213	
214	
215	Fuck this technology. Fuck shotspotter. Fuck SPD. Fuck SPOG. When will you listen to the people of this city? We do NOT trust SPD or SPOG and never will. There needs to be a major overhaul in Seattle regarding "law enforcement". We should be a leading city when it comes to this, we should live up to our reputation. But instead we hide and cower and think state-sanctioned gangs will keep us safe. WE keep us safe.
216	
217	Privacy and time of when spd deletes the information. Should be able to follow other cities if this moves forward (which it should not).
218	
219	
220	Read 1984.

Question 7: Do you have any additional comments or questions?

ID	Do you have any additional comments or questions?
1	I think it's good that SPD is aggressively going after stolen property. I just don't want the database to come back to haunt us, so more policy control over that should be implemented prior to the expansion.
2	
3	
4	

5	
6	
7	Quit being a libtard
8	
9	Is this only to be installed on vehicles or will there be stationary roadside cameras as well? What are the equity implications for neighborhoods that have more police vehicle traffic than others?
10	I understand that the issue at hand is increasing the use of this technology, but my honest preference is that its use be discontinued entirely.
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	Council recently told Seattle teachers there was no money to pay them a living wage during a period of historic inflation. Why are we even considering spending millions on Orwellian programs in light of that?
22	
23	
24	No
25	
26	Do not allow this in good conscience. As I write this, there have been three violent crimes in my neighborhood, per Citizen. I would rather there be more effort actually taking care of our neighborhoods. On foot. In real life.
27	
28	
29	I'm sickened that this is even being discussed. We're tracked enough; why add to the already crushingly demoralizing feeling of living in a world that monitors people's every breath?
30	
31	No
32	
33	For the people, by the people!
34	
35	
36	
37	
38	
39	n/a
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	The issue is public safety in the global use of the term. While implementation and use of the proposed technology is re-active, it is an opportunity to prevent follow-on criminal activity, recover individuals and property, reduce road rage, etc. Law enforcement clearly understand the issue. Supporting data goes back decades. An independent agency along with the justice department, not city leadership, needs to be authorized to review all historical data (including abuses associated with the technology), communicate with others currently using similar systems,

	specifically define the desired outcome, assess implementation with appropriate guardrails, transparently communicate with the public - including annual or semi-annual reporting of outcomes of the use of the technology, any abuses and means to prevent further abuses, lessons learned.
50	
51	
52	no
53	
54	
55	
56	I wish the city council to know this will absolutely effect my vote in future elections. I will not vote for anyone who supports this technology.
57	
58	acab
59	Never increase police surveillance. Always protect citizen privacy.
60	
61	
62	
63	
64	
65	
66	
67	
68	People will be murdered as a direct result of this. Most of the murder victims will be women.
69	
70	
71	
72	
73	
74	
75	Defund the police. Fund human services.
76	
77	
78	
79	
80	
81	
82	it is terrifying that this proposal was allowed to advance this far.
83	
84	
85	
86	
87	
88	
89	
90	Don't give the cops anymore expensive toys to invade our privacy.
91	
92	I have concerns for undocumented immigrants with this system.
93	
94	None
95	
96	
97	

98	
99	This will make things even more dangerous for victims of abuse and dv!!
100	
101	
102	
103	
104	Additional comments: Do not coddle poor drivers!
105	
106	
107	
108	
109	
110	
111	
112	
113	
114	
115	Please invest money in important systems! It is embarrassing that SPS is in such a funding defect and instead of supporting and uplifting the youth of Seattle, you are only creating things that will make it less welcoming for them.
116	
117	
118	
119	What will keep anyone on the internet from downloading a copy of this database on a periodic basis, creating essentially a permanent record potentially spanning years of all vehicles' data that is recorded? How robust is the authentication system that may be used to protect the database from download?
120	
121	
122	Tell Them "Nyet Comrade".
123	
124	
125	Why aren't you arresting people for committing crimes?
126	
127	
128	
129	
130	
131	
132	This is police overreach and a response in the form of a ballot measure will likely follow if city leadership doesn't address this promptly
133	
134	No, shame on the SPD for investing in this technology
135	
136	Considering the past decision from the city council on police enforcement policies, I am hoping that they have learned their lessons and that public safety is one of the top issues right now in the city.
137	
138	
139	
140	
141	
142	
143	
144	
145	

146	
147	
148	Everyday this week somebody is shooting in the CD - we are living in the middle of a gang war and it's just a matter of time before a stray bullet kills (another) person who isn't involved in the gang war.
149	
150	Why do you think this is a good idea?
151	
152	
153	No, this covers it. I have work to do and shouldn't even have to be doing this survey. It should be common sense that we need police that look a lot like they do in other developed countries.
154	
155	
156	
157	None right now.
158	Stop giving the police more resources and put them back into the community
159	
160	
161	
162	
163	
164	None
165	It makes me very proud of this city that I am able to submit my concerns for consideration. I thank city leaders for their time.
166	This is a terrible idea, don't waste our collective tax money on this.
167	
168	
169	Please vote NO on APLR
170	
171	
172	
173	I hope the results of this questionnaire are available via FOIA.
174	
175	
176	
177	
178	
179	
180	When I'm out and about in public I may not have any reasonable expectation of privacy. However there's no need to make it easy for outside people to track me down. Since New Hampshire proved it's possible for this system to work when purging unneeded photos every 3 minutes, there's no possible reason for SPD to keep my pictures for 3 months.
181	
182	
183	
184	
185	
186	
187	
188	
189	
190	
191	
192	
193	

194	Just found out about this survey today, this is the concern about transparency and info access.
195	Yes: what of the six Seattle Police Department officers who were found to be on the National Mall during the January 6, 2021 riots in Washington, DC?
196	
197	
198	Do not expand this technology to any new vehicles. Do not retain any data related to non-hits for a period longer than 3 minutes. If that is not possible, do not collect and retain it at all. If it is to be collected it should only be retained the period minimally feasible, and in no wise for longer than an hour, otherwise just don't do it. At all. Period.
199	
200	
201	
202	
203	
204	
205	
206	
207	
208	
209	
210	
211	Stop the sweeps, any problem caused by a person living in a tent or a car can be addressed without forcing them to move
212	
213	
214	
215	Don’t pass this. This is gross and disgusting and scary. My communities do not have good relations with police and this will only worsen it. If you want to gain the respect and trust of Seattlites, please listen to us. Otherwise I imagine folks will continue to fight this and take it to the streets.
216	
217	
218	
219	
220	

City of Seattle

ALPR Public Comment received via Privacy Inbox

December 9, 2023

cc: Seattle IT / Privacy

Dear Seattle Council Members Juarez, Morales, Sawant, Mosqueda, Herbold, Nelson, Lewis, Peterson and Strauss;

WA People's Privacy is offering this letter to you all with deep concerns over the proposal to vastly expand the use of Automated License Plate Reading (ALPR) technology in Seattle across several city departments. We also want to acknowledge the timing of this letter: this is happening just after Seattle City Council members have approved the purchase of Sound Thinking (formerly named ShotSpotter) audio surveillance technology and integrated CCTV cameras, *and* after it passed a Ceasefire resolution. We are disappointed to see Seattle continuing to deepen and expand city-wide surveillance of residents and visitors rather than using those funds to secure the real and tangible safety of its most precarious residents, such as provisional housing and care for unhoused and housing-precarious people, increasing hunger and food security supports, and an expansion its emergency sheltering and resource provisioning capacity. We also urge City Council members to consider whether their positioning is performative or real when it comes to calling for a *decrease* in violence against citizens in other parts of the world, while pursuing *increased* violence against people at home in Seattle by expanding policing and surveillance powers. Surveillance isn't safety,[1] and if everyday violence in U.S. cities does not demonstrate this well enough for Council members, #Gaza is a solid and truly devastating example of the fallout of invasive surveillance and state control on fast-forward.

While it's clear that ALPRs appeal to police and cooperating agencies in that they provide broad and easily trackable data about any and every car's travels throughout the city, state, and nation; this technology poses acute and disproportionate threats to many communities, including immigrants, abortion and gender-affirming care seekers, and Black and Brown people and communities. But, ALPRs actually pose great risk to everyone's first and fourth amendment rights,[2] and thus all people's safety and security.

It's our understanding that SPD is looking to purchase and expand the use of AXON 3 ALPR cameras to its entire fleet and across departments. After review of the promotional content and videos for AXON products, it's clear that AXON interfaces with a suite of other surveillance technologies and platforms, including body cams and the import of ALPR data from other sources. AXON systems include interview recording technologies, surveillance cameras, now the use of AI for both face recognition and ALPR technologies, and more. Via AXON's software, ALPR data can be integrated with many other kinds of data. As long as inter-local agreements are in place, ALPR and other data can be easily shared across local, state and federal agencies with a few clicks in the software platform. Whether it's AXON or another company, ALPR providers have similar features in order to compete in the law enforcement tech marketplace, so the brand or company itself is less important than the overall functionality and harms of this tech in general.

ALPR technology does not operate in a vacuum. The data ALPRs collect can be stored, including in agency case files as evidence (once marked as evidence, much longer retention periods apply for any kind of data agencies collect), added to various lists –including "hot lists," and shared. With their focus on broadening and expanding their surveillance products and profits, **private companies often include**

[1] https://truthout.org/articles/surveillance-technologies-dont-create-safety-they-intensify-state-violence/

[2] https://www.independent.org/news/article.asp?id=14516

"**Community Addition" features.** These enable additional parties, such as neighborhood surveillance groups, businesses/corporations and other third parties to offer up *their* ALPR or other surveillance data for import into the law enforcements' existing systems and integrate it with that data. Sometimes this additional data is sourced from from Lexis Nexis via other agencies,[3] Flock,[4] (See also ACLU's alert on Flock[5]) or other sources – such as Motorola's Vigilant Solutions.[6] *Community addition features, as well as the availability of all city ALPR data for 90 days via records requests, present many harms, and a what many legal scholars regard as a dangerous run-around of our fourth amendment rights.*

City Councils should thoroughly investigate the various integrations and cross-platforming of SPD's surveillance technologies, and the ways in which their data storage and sharing settings, including inter-local sharing agreements, may be dangerously invasive for Seattle residents and visitors alike. According to AXON's video describing feature updates in December 2023 and coming in March of 2024, AXON 3 ALPR cameras function up to a 75-foot distance, in all lighting conditions, and captures as many as 75 plates at once/per minute. AXON's server and cloud-based systems are set up to retain and share large amounts of data, with the ability to share/transmit 100,000 pieces of evidence to another agency in one "share" or transmission. The University of WA Center for Human Rights produced a detailed report last December on the dangers of ALPRs, specifically detailing the dangers to immigrants and abortion seekers Post-overturn of Roe v. Wade.[7] However, threats to the public are actually far more expansive. The end of that report offers specific recommendation to policy makers, which generally overlap with WA People's Privacy's recommendations to you here.

Threat of harm to abortion and gender-affirming care seekers:

In the wake of Roe's overturn in our 2023 session, our WA State Legislature enacted a shield law that *should* prevent WA State agencies from cooperating with law enforcement investigation requests to prosecute people for seeking abortion and gender-affirming care here, however; we have recent news that Oregon's similar shield law has already been worked around via location data obtained without the cooperation of Oregon agencies.[8] The more data collected on people, the less safe we are from this kind of tracking. As the recent Stranger article[9] aptly points out: with a planned retention period of 90 days, ALPR data from Seattle's systems would not only be accessible for periods long enough to allow ethics-compromised officers to help officers from out of state abuse that access, but also via public records requests. This means our shield law may *easily* be thwarted by out of state actors in collaboration with in state residents, none of whom need be law enforcement status in order to obtain the records and then offer them up to law enforcement in other states. There are plenty of extremely dangerous individuals and communities looking to harm abortion and gender-affirming care seekers, *this is not a hypothetical.*

---

[3] https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/

[4] https://www.newsobserver.com/news/state/north-carolina/article281363348.html

[5] https://www.aclu.org/wp-content/uploads/publications/flock_1.pdf

[6] https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations

[7] https://jsis.washington.edu/humanrights/2022/12/07/whos-watching-washington/

[8] https://www.theguardian.com/us-news/2023/nov/01/idaho-mother-son-kidnap-charges-abortion

[9] https://www.thestranger.com/cops/2023/12/05/79293457/seattle-police-department-pitches-dramatic-expansion-of-vehicle-surveillance

Threat of harm to immigrants:

The risks of ALPRs to immigrants has been an ongoing discussion for years. As Georgetown's Immigration Law Journal explained clearly in a 2020 article: this data can and has been used to target immigrants.[10] Similar to shared above, the dangerous tracking and targeting of immigrants is not simply a threat by far-right and xenophobic LE agency actors, but also by hostile individuals and groups seeking to harm immigrants. In our current climate of increased threats of violence to Muslim, Jewish, and Sikh communities and individuals amid what UN officials have characterized as a textbook case of genocide in Gaza by Isreal; the threats to safety that this kind of data and its extended retention and availability to the public presents *cannot* be allowed to occur in Seattle, or in our State.

Threat of harm to all people exercising our First Amendments rights to speech, public protest & assembly:

As Seattle leadership and police are keenly aware, Seattle has a strong tradition of participatory democracy, public assemblies, and protest/demonstrations for or against particular issues. One of those issues has been policing. During the mass uprisings against police murders and violence, Seattle residents utilized their First Amendment rights to make strong statements not only to decry police violence in all its forms, but also to envision a city without invasive policing and mass surveillance. Seattle's also seen mass demonstrations around abortion rights, international trade policies and conventions, pro-peace / anti-war demonstrations, protests to sweeps, and even a recent interfaith coalition calling for a ceasefire in Gaza. Outfitting every squad car with ALPR cameras will exponentially increase risks to people exercising our rights to speech. Again, ALPR data does not exist in a vacuum. It can be integrated with body cam footage, and other camera footage in place of public egress, in addition to a web of private surveillance camera footage –all accessible to law enforcement. Not only can people offering up their dissent in a public place be tracked and targeted based on photographs, but now so can their cars, and then all of their subsequent travels.
ALPRs pose safety risks and threat of police retaliation to people exercising our rights to speech, particularly in a political environment that has become increasingly polarized and threatening to many people of marginalized identities and communities.

Threat of harm to women, sexual assault and stalking survivors, and vulnerable/marginalized populations:

Countless organizations have flagged ALPRs as not only objectively invasive of privacy, but as extremely dangerous to victims of stalking, harassment and intimidation. In a publication of the University of Michigan's Ford School of Science, Technology and Public Policy,[11] they flag these threats, and note that several cities have banned the use of ALPRs completely due to the increased threats of violence they open up for vulnerable people. Officers have misused databases for personal abuse,[12] and professional abuse has targeted people based on religion and race/ethnicity. While women make up the majority of cases of stalking, LGBTQ+ people are also at increased risk. This population includes people facing poverty and extreme precarity, in addition to sex workers, who often face extreme threats to their safety, including from law enforcement targeting, in addition to the many state harms due to the marginalization and

---

[11] https://stpp.fordschool.umich.edu/news/2023/automated-license-plate-readers-widely-used-subject-abuse

[12] https://www.kwch.com/2022/10/31/kechi-police-lieutenant-arrested-using-police-technology-stalk-wife/

vulnerabilities they face. Bottom line, no one deserves to be stalked, assaulted or harassed, and we don't need to be employing tech and surveillance that further enable such violence.

The risks of the use of ALPR technology far outweigh its benefits. If the City Council fails to regulate on this and allows for the expansion of this technology, which we hope it will not given all of the concerns listed above; WA People's Privacy suggests that the following steps be taken and legislated by the City Council to mitigate some of its harm.

1. Delete all ALPR data collected – that is *not* a direct hit on a "hot list" in pursuit of an abducted person or a violent offense – within 48 hours.

2. Do not allow parked SPD vehicles to use ALPR functionality anywhere in the vicinity of a public assembly or protest. Require that ALPRs on any vehicle in the vicinity of a public assembly or demonstration be shut off or in sleep mode, and require regular audits after every public demonstration event that SPD vehicles have been in the vicinity of, or mobilized intentionally to, in order to ensure adherence with people's First and Fourth Amendment rights.

3. Ensure that policy and use agreements with the vendor are modified to ensure the privacy and protection of Seattle residents and visitors.
   a. Review vendor data retention policies and ensure a negotiated contract with AXON that adheres to a 48-hour ALPR deletion policy from *their* data storage that is in line with Seattle's 48 hour deletion policy. Third parties are not beholden to rules governing SPD ALPR use, unless they are pro-actively negotiated and in writing.
   b. Review AXON's policies on sharing data, and revise contract and policy language as needed to ensure that ALPR data cannot be shared by any other party except for it's collecting agency (no third party sharing or selling by AXON or its affiliates).
   c. Review AXON's integration policies and ensure that ALPR data is not being used in a way that amplifies it's surveillance footprint, such as being used alongside face recognition, Flock or Sound Thinking (formerly ShotSpotter) Audio and CCTV Surveillance, without new and additional review of such by the Seattle Council and the public.

4. Call for an independent audit and review all integrations and inter-local sharing agreements that have access to or can be combined with ALPR data to ensure that SPD cannot and is not in violation of Shield Laws, whether willfully or unknowingly.

As Seattle navigates proposed uses of different technology in various ways, it is essential that our lawmakers center people's constitutional rights, and conduct diligent inquiry into the harms of new and expanded technologies. We urge our council members to resist rosy-sounding marketing spiels of companies looking to not only profit off of the invasion and violation of people's privacy, but to work with law enforcement to engineer a world in which every minute of people's lives is tracked, measured, searchable, and documented in data points that are endlessly shared/sold, and up for grabs by a network of agencies and corporations around the world. We cannot stress enough the broader implications of this kind of data surveillance to democratic governance, fair elections, and healthy participatory democracy.

Law enforcement will never advocate for *less* surveillance, nor *less* access to people's private lives. They never have. In fact, law enforcement departments and agencies will always advocate for *more* access, whether it's invasive and rights-violating or not. The private market is more than happy to meet those desires by pitching ever more invasive and harmful tech, and raking in the profits.

But, it is not the proper role of our lawmakers to be in league with law enforcement on that tendency. In fact, is not the job of lawmakers to make policing the public easy or privacy-violating at all. If anything, our legislators bear the opposite responsibility: that of upholding our constitution and the rights it affords, and attending to our human and civil rights *first* with each and every policy decision and law passed. Law enforcement and police are not entitled to define what safety is, nor how it is achieved. THAT is the purview of people and lawmakers.

Many of the technologies marketed to law enforcement agencies are first tested on occupied and vulnerable populations abroad before being marketed here in the U.S.[13] and it's vital that our lawmakers understand this. In a globalized economy, Seattle budget and surveillance decisions are very much connected to human rights and wars, global data flows and geo-politics.

WA People's Privacy calls on the the Seattle City Council to work *to roll back the use of surveillance tech* in Seattle, not to increase it.

While we were unavailable to engage with the Council in support of the community's recent call to stop the City's purchase of Sound Thinking with CCTV cameras (formerly ShotSpotter) this year; we are very concerned about the purchase and adoption of that tech. With our understanding of and expertise in data privacy issues, big data flows & commercial and law enforcement data surveillance, as well as the myriad of threats (local, state, national and global) to people's privacy, safety and security *and* our democracy that unchecked data surveillance currently creates, we would be remiss if we did not flag for the Council the compounding and intersecting harm that each additional form or surveillance tech adopted by the city creates for actual people.

An entirely unregulated industry is currently expanding and further deepening already-existent harms in tech with the integration of complex algorithmic software (AI). Similar to our note about what the new and updated AXON 3 ALPR Camera systems are capable of, the Council must be prepared to navigate proposed revisions/updates to all of its existing tech contracts that will pose much deeper privacy-invading harms and threats. We can guarantee that these proposals will continue to come before the Council, and it would be wise to either pause them and ask for State and Federal regulatory action first, or allow civil and digital rights experts and people's advocates to assist Council members in bringing forward proactive law to mitigate these imminent harms in advance. Increased data surveillance combined with big-data-powered AI features will present increasing and deepening harms and threats to *all* of us, but will be disproportionately aimed at targeted individuals and groups, including immigrants, healthcare-seekers, LGBTQ+ people, Black and Brown people, and anyone exercising our rights to speech in public.

We urge to you to proceed with an *over*-abundance of caution, to disallow the deepening and expansion of surveillance at a time when the U.S. has yet to legislate to protect people's rights in the area of mass data surveillance, and is still considering such legislation.

On behalf of WA People's Privacy, thank you for your time and review of this letter, and thank you all for your work. Please reach out with any questions.

Very truly yours,

Maya Morales, founder
WA People's Privacy

---

[13] https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/

Letter received via Privacy email inbox:

Dear Seattle City Leadership,

Here is my public comment on the Material Updates to the proposed new SPD Automated License Plate Reader (ALPR) Fleet-Wide Surveillance Impact Report (SIR).

Over-arching Top Concern: Data Retention of Non-Hits

A journal article assessing 87 days of SPD ALPR data collected in late-2012/early-2013 via both Patrol & Parking Enforcement (aka PIPS & AutoVu) found that in total SPD's ALPR systems scanned over 1.7 million license plates but only 9,660 of those plates were on a hotlist (aka a "hit"), which is only 1.2% of all plates scanned [1]. This percentage is largely bolstered via the Parking Enforcement ALPR system scanning less plates and being more likely to return a hit which for this dataset includes any ALPR data retained because it is associated with an SPD case; and since parking enforcement is more likely to scan plates that they then issue a parking citation for (SPD Patrol does not issue parking citations) and because there are more parking violations occurring than there are felonies, this means Parking Enforcement will generally be expected to always have more hits. But SPD's overall fleet of vehicles contains more patrol cars than parking enforcement vehicles, so it makes more sense to focus on the Patrol (PIPS) data. Drilling down into that, we see that most of the overall plates scanned (1.5 million) was from Patrol but only 3,775 were hits or 0.25% [1]. **This means that over 99% of the plates scanned by SPD Patrol and having their timestamped geolocation details retained for 90 days were just innocent people going about their day.**

According to the US Census, Seattle had a population of 608,660 people in 2010 and 737,015 in 2020 [2]. Though the Census counts include people too young to drive and people without cars, so those numbers are an over-estimate of the possible unique plate reads. Based on WA DOL data, we know that there were roughly 417,973 vehicle registrations in 2022 for King County (data not broken down to the city-level & only available for 2022) [3]. When Seattle's population was smaller SPD, still scanned nearly 3 times as many plates as there were residents. Some of those plates will be for non-residents, but it also seems very likely that unless you keep your car hidden in the garage and never drive it, that SPD has likely been tracking your location history; and there's no *technical* control in place that *prevents* the abuse of this data.

The long retention of reads that are not hits means **SPD's ALPR system currently meets the definition of mass surveillance** (aka "bulk collection")[4][5] and this problem will only be worse with the proposed expansion of this technology.

Seattle's Community Surveillance Working Group (CSWG) in their Privacy & Civil Liberties Impact Assessment recommended limiting retention of ALPR read data for non-hits to at most 48 hours. Seattle City Council specifically passed an amendment seeking to reduce the data retention of non-hits to 48 hours, inline with the CSWG. SPD's response was that their "position on this issue is guided by the operational practicalities of criminal investigations which cannot be confined nor defined by a static time frame, in part, due to the various constitutional protections and safeguards law enforcement must adhere to in investigating." But the request for the 48 hour retention period only applies to non-hits, meaning the data was not associated with a criminal investigation, so the shorter retention period has no impact on the data retained for investigations; and it would also have no impact state or federal "constitutional protections" or "safeguards". SPD goes on to state, "SPD simply does not have the capabilities to resolve questions of whether the data is case related within 48 hours, and any such retention period is therefore wholly unfeasible." If this is true, then this would mean that SPD believes they are less capable than multiple other police departments considering that New Hampshire

only retains non-hits for at most 3 minutes. **So every single police department in the entire state of New Hampshire can somehow manage to avoid conducting mass surveillance of their residents and yet New Hampshire hasn't devolved into a lawless state that criminals flock to - calling into question then SPD's supposed justification.** Even Axon's default data retention period for ALPR reads is one-third (30 days) the amount of time SPD says they need [6]. This leaves the public facing only one of only two (unfortunate) possible options then: doubting SPD's workmanship or their integrity.

Since location data by it's very nature contains information about people's everyday life movements (where they live, work, worship, receive healthcare, etc), it can be easy to find patterns in the data. This is what makes location data exceptionally hard to truly anonymize. In 2013, researchers confirmed that location data is highly unique to a person. They analyzed anonymous location data on 1.5 million people and found that **"four spatio-temporal points are enough to uniquely identify 95% of the individuals"**. They went on to say, "We showed that the uniqueness of human mobility traces is high... Indeed, this uniqueness means that little outside information is needed to re-identify the trace of a targeted individual even in a sparse, large-scale and coarse mobility dataset"[7]. Here within the SPD ALPR dataset, this likely means that a person seeking to re-identify a target person doesn't need to already know their license plate number or have access to the DOL database that has this information. SPD's ALPR database is effectively not anonymous.

Chronological Breakdown of Concerns About the Updated SIR

SIR page 6 - Incorrect Information: Data Storage

- Item 2.3 in the updated SIR states, "No ALPR data collected by SPD are automatically uploaded into any system outside of SPD." which is incorrect since Axon Fleet 3 inherently entails storing the ALPR data off of the SPD network and not on SPD-managed hardware. Instead Axon states that, "Both read and hit records are generated in the Fleet 3 Hub and temporarily stored there before uploading. ... Copies of read and hit records are stored on the hub for 24 hours. Both read and hit records are uploaded to the agency's Axon Evidence cloud storage..."[8]. This erroneous sentence in 2.3 of the updated SIR seems to be due to SPD forgetting to remove that text considering the old system (Neology PIPS) wasn't cloud-based and the signed ordinance for the original SIR states, "All data collected by the Patrol ALPR systems (images, computer-interpreted license plate numbers, date, time, and GPS location) are stored on-premises on a secure serve..." which was (correctly) removed from the updated SIR. However, this erroneous sentence seems to have been forgotten to be removed resulting in the description of the technology in the SIR being inaccurate.

SIR page 7 - Missing Information

- A potentially concerning section of item 2.5 has been removed in the updated SIR. Specifically, the text from 2.5 that SPD is no longer adhering to is:
  - "The Technical and Electronic Support Unit (TESU), a unit within SPD maintains administrative control of much of SPD's physical technology. The unit staff is knowledgeable about investigative and forensic technology. TESU's mission is to provide technical assistance to Detectives and Officers in connection with investigations. The BOSS ALPR administrator is a member of TESU. The ALPR administrator monitors and manages user access to the PIPS ALPR system for Patrol. The ALPR administrator purges users from system access when they leave the Department. Housing management of the Patrol ALPR system in one unit makes oversight and accountability more efficient than tasking individual units or precincts with this themselves."

- Of course it's expected that references to BOSS and PIPS would need to be removed but SPD hasn't replaced this information with equivalent information for the proposed new Axon-based setup. And we know there is still a role held by someone/some-team of "ALPR administrator" since item 3.2 mentions "A record of these requests is maintained by the ALPR administrator." But with details in 2.5 removed, the public has no idea regarding the complexity (and therefore safety) of the revised SPD ALPR system, which results in multiple open questions:
  1. Does this mean that every SPD department will have their own ALPR administrator?
  2. Or is it perhaps one ALPR administrator per precinct?
  3. Does this also mean that maybe every department or precinct will provide their own ALPR training, not a unified approach?
  4. Is the ALPR administrator even an SPD employee and instead Axon does all the administration?

  The public shouldn't have to guess since this is supposed to be addressed via item 2.5.

SIR Page 8 - Missing Information: Limitations on Use

- Item 3.2 in the updated SIR removes the explicit list of conditions under which SPD's ALPR can be used. Since 3.2 asks the department to "List the legal standards or conditions, if any, that must be met before the project/technology is used", those specific limitations need to be listed inside the SIR itself (not solely in an outside document subject to the changing whims of SPD and not providing the Council oversight required via the Surveillance Ordinance, SMC 14.18.040.B.3.b [9]). This is especially important considering the SPD Policy referenced in item 3.2 (16.170-POL) assumes that the only systems being managed were less than two dozen vehicles and having two different yet specific solutions (PIPS vs AutoVu) [10]. One would assume that 16.170-POL will be updated if/when the updated SIR is approved by City Council; however, in that future policy editing process, the revised policy should not be worse at protecting residents due to lack of details in the SIR. **The SIR must contain the explicit limitations on the use of ALPR, and the SPD Policy should then follow the requirements laid out in the SIR (not the reverse).**

SIR page 8 - Missing Information: ALPR-specific Training

- Item 3.3 asks the department to "Describe the ... training required..." but SPD's answer in regards to this specific surveillance technology was "The policy requires that users must be trained" and the certifications they must hold. However, that does not explain anything regarding the training for this system; resulting in multiple open questions:
  1. Who conducts this training, Axon or SPD?
  2. Does this training only consist of how to use the system for daily needs and not civil liberties or privacy-related content (such as being explicitly instructed to never use the ALPR system for personal purposes, like searching the geolocation history of your ex-gf/wife, neighbor you don't like, etc; or staking out parking areas for your own personal interest, like gay bars, synagogues, strip clubs, etc)?
  3. How often does this training occur?
  4. Does an OIG or OPA investigation (regardless of outcome) that included the use of ALPR systems necessarily require employee re-training on the use of ALPR and the policies/laws around it's use?
  5. Who creates the training content?
  6. How often is the training content updated?
  7. Is the training content updated when there's been an OIG or OPA investigation (regardless of outcome) that included the use of ALPR systems?

  Again, the public shouldn't have to guess since this should to be in item 3.3.

SIR page 9 - Missing Information: Searching the ALPR Database

- Item 4.3 only describes the deployment, not all of the usage of the system. Specifically, item 4.3 does not address searching the ALPR database; resulting in multiple open questions:
  1. Who will have access to search the ALPR database?
  2. Can searching of the ALPR database be done within an SPD vehicle or does the person need access to, say, specific workstations on SPD premises in order to run search queries against the ALPR database?
  3. Do only certain departments or work roles have access to run searches; or can all SPD employees search the ALPR database?
  4. How many SPD employees will have access to the "Record Search" tab of the ALPR database in Axon?
  5. How often are searches conducted against the ALPR database?
- **Since searching through the historical records in the ALPR database is where most of the privacy and civil liberties issues are encountered, it's very important that this workflow of using the system is answered by SPD inside the SIR.**

SIR page 9 - Missing Information: Scale of Deployment

- Item 4.6 previously gave a tally of the marked and unmarked ALPR-equipped vehicles. SPD is now withholding information from the public regarding both how many total SPD vehicles have in-car video (and thus are on deck for ALPR) and how many out of those are unmarked vehicles. There's no valid reason to withhold this information from the public since any notation on the number of vehicles can specify the current count as of the date the update SIR was drafted, especially since the updated SIR repeatedly states the scope is "fleet-wide". **The lack of this critical information hinders the public's ability to accurately assess the pros and cons of the proposed fleet-wide roll-out.**

SIR page 10 & 11 - Potential Security Weakness

- Since SPD is moving from an on-premise to cloud-hosted solution, the answer to items 4.10 and 5.1 are arguably even more important now. SPD's answer mentions the use of login credentials (assumed by the public to simply be a username/password pair, without two-factor authentication) and SPD has removed discussion about the software systems access. This leaves open questions about the security & privacy of the data stored within Axon:
  1. Are the reads that are recorded in the ALPR database encrypted and specifically is that using client-owned/-managed (SPD owned/managed) encryption key(s)?
  2. Does Axon have technical access to the raw ALPR data generated from SPD vehicles?
  3. If Axon's network were to be security breached, what technical safeguards are present to render useless to an outsider the ALPR data generated by SPD vehicles (such as hashing and client-side encryption prior to uploading to Axon)?
  4. Additionally, Axon's Privacy Policy says they employ "other companies and people to perform tasks on [their] behalf and may need to share your information with them to provide products or services to you" [11], so what *technical* (not legal) safeguards *prevent* a rogue Axon employee or a rogue employee of a contracted company by Axon from accessing, searching, or sharing externally the ALPR data generated by SPD vehicles?

SIR page 11 - Missing Information: ALPR Audits

- In item 5.2, SPD says, "SPD conducts periodic reviews of audit logs and they are available for review at any time by the Seattle Intelligence Ordinance Auditor under the City of Seattle Intelligence Ordinance." With that in mind:

1. **When was the last audit conducted of SPD's existing ALPR systems?**
2. **Within the last 5 years, how many violations of 16.170-POL were detected based on review of the ALPR audit logs?**

- A functioning audit system (logs & human workflows) should over the course of a few years detect at least a small number of mis-uses of a system (irregardless if the reason was for say efficiency's sake in the moment or personal gain or another reason). So if SPD's auditors reply back that there's been zero violations detected, then that implies that the auditing system is not working.

SIR page 11 & 12 - Incorrect Information: Data Storage & Sharing

- Item 6.1 contains the erroneous sentence, "No person, outside of SPD, has direct access to the PIPS system or the data while it resides in the system or technology." That sentence is wrong for two reasons: first of course being that Axon Fleet 3 is the ALPR system the updated SIR is supposed to be describing and secondly because SPD is moving from a on-premise to cloud-hosted solution which means it is not true that "No person, outside of SPD, has direct access" to the ALPR data, since Axon would have access. This is true even moreso if SPD is not using client-side encryption, which would mean that Axon (including some of its employees) has technical access to all the raw ALPR data SPD generates.
- Also related to item 6.1, Does SPD currently or plan to use Flock Safety, which is a data sharing partner of Axon Fleet?

SIR page 15 - Misleading Content

- SPD's answer to item 7.3 misguides the public by stating, "Because SPD's fleet-wide ALPR cameras are not fixed in location and records are only retained for 90 days, privacy risk is substantially mitigated because of the limited ability to identify vehicle patterns." SPD is proposing increasing the number of ALPR-equipped vehicles from 19 to roughly 300, which is over 15 times more vehicles than currently. Moreover, Axon's website states, "The Axon Fleet 3 ALPR system utilizes a wide field of view (60°) covering 3 lanes out to 50 feet in front of the vehicle. So, while a traditional ALPR system with 2 forward facing cameras has a detection area of approximately 192 cu. feet, Axon ALPR detection area is approximately 90 times that area"[12], so each ALPR-equipped vehicle will also be able to cover roughly 90 times the visual scanning area of the current SPD ALPR-equipped vehicles. 90 days of read data is already more than enough data to re-identify most individuals in such a location dataset (see prior introductory discussion about only needing 4 timestamped location data points to re-identify 95% of people), so the statement by SPD that there's "limited ability to identify vehicle patterns" is not substantiated by any data from them and is on its face obviously untrue given the scale of the ALPR data they're already collecting. Item 7.3 specifically asks, "describe the privacy risks identified and for each risk, explain how it was mitigated"; but **a 15 to 90 times greater (or more) amount of scans possible is not a "mitigation" of a privacy risk - it's the exacerbation of the existing risks.**

SIR page 17 - Missing Information: Cost

- The Fiscal Impact section is blank in the updated SIR, so the public has no idea:
  1. How much the initial acquisition & installation of these cameras will cost?
  2. How much they are expected to cost to maintain?
  3. How much are the recurring costs (like the subscription to have the ALPR data stored in the cloud or licensing fees)?

SIR page 20 - Missing Information: ALPR is a Surveillance Technology

- In item 1.1 of the RET in the updated SIR, SPD has unchecked all the boxes, which means according to SPD they feel their ALPR systems don't meet the criteria in the Surveillance Ordinance of being a surveillance technology. Surely this must be a mistake that the the third box is now unchecked.

SIR page 21 - Missing Information: Civil Liberties Concern

- In item 1.2 of the RET, SPD has removed the potential impact of, "An additional potential civil liberties concern is that the SPD would over-surveil vulnerable or historically targeted communities, deploying ALPR to diverse neighborhoods more often than to other areas of the City." This concern still exists. In fact having more SPD vehicles with ALPR systems only makes this potential worse, since if there are more vehicles canvassing certain neighborhoods over others, then there will be potential disparities in which innocent bystanders are more aggressively surveilled in SPD's ALPR data.

SIR page 25 - Misleading Content; No Organization Outreach

- In item 1.7 of the RET, SPD says "90-day data retention also mitigates the risk of improper identification of community members"; however, 90 days is more than enough data points to accurately re-identify a person (see prior introductory discussion about only needing 4 timestamped location data points to re-identify 95% of people). This is especially true given that the existing system scanned over 1.7 million plates back in 2013, but with a larger population and a 15 to 90 times greater coverage of plates scan in the proposed fleet-wide system, there will certainly be vastly more plates being scanned and more scans-per-plate. Thus this new much larger, more pervasive system also having a 90 day retention period for non-hits makes it that much easier to re-identify individuals - again, **this is not a "mitigation" of a privacy risk - it's the exacerbation of the existing risks.**
- According to item 2.1 in the RET, zero organizations were specifically invited to provide feedback on this updated SIR. It's unclear to the public if this was the responsibility of SPD vs Seattle IT, but someone should have been responsible for notifying local organizations (presumably at the bare minimum the six organizations notified in the original ALPR for Patrol SIR).

<u>Priority Order of Recommendations</u>

1. Only retain data on ALPR reads that are non-hits for at most 48 hours.
2. Add all the missing information into the SIR.
3. Remove misleading information from the SIR.
4. Conduct outreach to local organizations notifying them of this Material Update.
5. Correct any the incorrect information in the SIR.
6. Correct any security weaknesses in the implementation.

Please seriously consider my public comment.

References:

[1] See pdf page 31: https://bpb-us-w2.wpmucdn.com/wpsites.maine.edu/dist/d/46/files/2014/06/03-Newell.pdf
[2] https://www.census.gov/quickfacts/fact/table/seattlecitywashington/PST045222
[3] https://fortress.wa.gov/dol/vsd/vsdFeeDistribution/DisplayReport.aspx?rpt=2022C00-62.csv&countBit=1

[4] "Thus, mass surveillance is indiscriminate, by definition. It involves methods that sweep up the data and communications of the entire population, notably including those of innocent people." ... "By contrast, targeted surveillance is portrayed as the collection of the data and communications of those who are considered to be the legitimate targets of government investigation and repression." from https://journals.sagepub.com/doi/abs/10.1177/0163443716643006
[5] "Based in part on briefings from the IC [Intelligence Community], the committee adopted a definition better suited to understanding the trade-off between civil liberties and effective intelligence: If a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted." from https://www.microsoft.com/en-us/research/uploads/prod/2019/09/Bulk-Collection-of-Signals-Intelligence.pdf
[6] https://my.axon.com/s/article/Fleet3-ALPR-FAQs?language=en_US#Q27
[7] https://www.nature.com/articles/srep01376
[8] https://my.axon.com/s/article/Fleet3-ALPR-FAQs?language=en_US#Q26
[9] https://library.municode.com/wa/seattle/codes/municipal_code?nodeId=TIT14HURI_CH14.18ACUSSUTE_14.18.040SUIMRERE
[10] https://public.powerdms.com/Sea4550/tree/documents/2042814
[11] https://www.axon.com/legal/privacy-policy
[12] https://my.axon.com/s/article/ALPR-overview-Fleet-3?language=en_US

Appendix C: Public Comment Demographics

Material Update ALPR Public Comment: Received via Microsoft form

Optional Demographics:

Age Range:

9. OPTIONAL Demographic Question: Age Range

More Details

Prefer not to identify	16
Under 18	0
18 - 44	113
45 - 64	51
65+	15

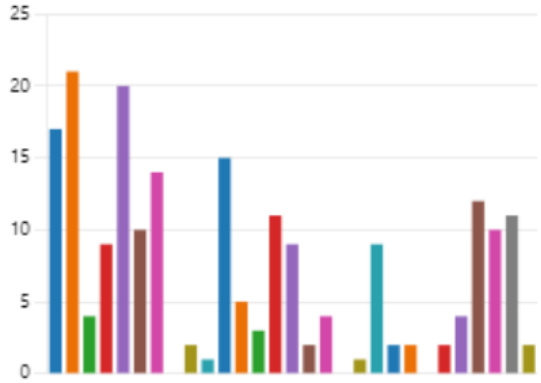
City of Seattle

Optional Demographics: Neighborhood

10. OPTIONAL Demographic Question: Neighborhood

More Details

Prefer not to identify	17
Ballard	21
Belltown	4
Beacon Hill	9
Capitol Hill	20
Central District	10
Columbia City	14
Delridge	0
First Hill	2
Georgetown	1
Greenwood / Phinney	15
International District	5
Interbay	3
North	11
Northeast	9
Madison Park/ Madison Valley	2
Magnolia	4
Queen Anne	0
Rainier Beach	1
Ravenna / Laurelhurst	9
South Lake Union	2
Southeast	2
Southwest	0
South Park	2
Uptown	4
Wallingford / Fremont	12
West Seattle	10
King County	11
Outside King County	2



Optional Demographics: Gender

11. OPTIONAL Demographic Question: Gender

More Details

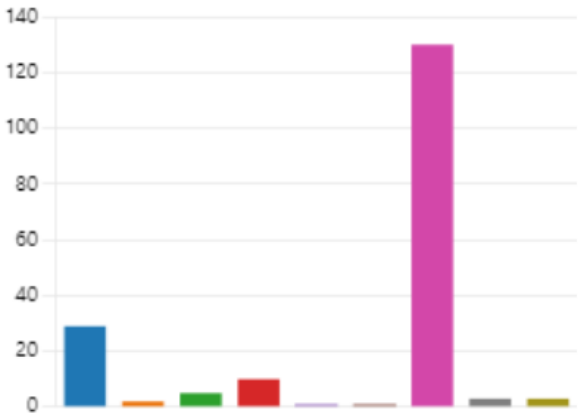
Prefer not to say	35
Woman	56
Man	76
Non-binary	14

Optional Demographics: Race / Ethnicity

12. OPTIONAL Demographic Question: Which race (s) / ethnicity (or ethnicities) do you identify as

More Details

Prefer not to identify	29
Black / African American	2
Hispanic / Latino	5
Asian / Asian American	10
Native Hawaiian or Pacific Island...	1
Indigenous	1
White or Caucasian	130
Another race/ethnicity	3
Other	3



Appendix D: Comment Analysis Methodology

Please refer to the original SIR (CB 120025).

Appendix E: Questions and Department Responses

Please refer to the original SIR (CB 120025).

Appendix F: Public Outreach Overview

Please refer to the original SIR (CB 120025).

Appendix G: Meeting Notice(s)

Please refer to the original SIR (CB 120025).

Appendix H: Meeting Sign-in Sheet(s)

Please refer to the original SIR (CB 120025).

Appendix I: All Comments Received from Members of the Public

Please refer to the original SIR (CB 120025).

Appendix J: Letters from Organizations or Commissions

Please refer to the original SIR (CB 120025).

Appendix K: Supporting Policy Documentation

Please refer to the original SIR (CB 120025).

Appendix L: CTO Notification of Surveillance Technology

Please refer to the original SIR (CB 120025).