From: Seattle Community Surveillance Working Group (CSWG)
To: Seattle City Council
Date: April 23, 2019
Re Privacy and Civil Liberties Impact Assessment for Automated License Plate Recognition, Parking Enforcement Systems, and License Plate Readers

## Executive Summary

On March 28th, 2019, CSWG received the Surveillance Impact Reports, or SIRs, for the three Automated License Plate Reader (ALPR) surveillance technologies included in Group 1 of the Seattle Surveillance Ordinance technology review process (Automated License Plate Recognition, Parking Enforcement Systems, and License Plate Readers). This document is CSWG's Privacy and Civil Liberties Impact Assessment for those technologies as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Councils.

This document first details the civil liberties concerns regarding ALPR surveillance technologies in general, and then provides specific concerns and recommendations for each of the three specific ALPR technologies under review.

Our assessment of the ALPR surveillance technologies focuses on three key issues:

1. The use of these systems and the data collected by them for purposes other than those intended.
2. Over-collection and over-retention of data.
3. Sharing of that data with third parties (such as federal law enforcement agencies).

For all three of these systems, the Council should adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

1. The purposes of ALPR use must be clearly defined, and operation and data collected must be explicitly restricted to those purposes only.
2. Dragnet, suspicionless use of ALPR must be outlawed.
3. Data collected should be limited to license plate images, and no images of vehicles or occupants should be collected.
4. Data retention should be limited to the time needed to effectuate the purpose defined.
5. Data sharing with third parties must be limited to those held to the same restrictions as agency deploying the system.

## Background: Civil Liberties Concerns with ALPR Systems

Automated License Plate Reader (ALPR) systems are powerful surveillance technologies that can significantly chill constitutionally protected activities by allowing the government to create a detailed picture of the movements—and therefore the lives—of a massive number of individuals. At the first public meeting seeking comment on the SPD Patrol ALPRs held on October 22, 2018, SPD stated that the ALPR system collects 37,000 license plates in a 24-hour period—which equates to over *13.5 million* scans over a full year. These drivers are not specifically suspected of any crime, which calls into question the scale and purpose of such data collection.
ALPR use creates a massive database of license plate information that allows agencies to comprehensively track and plot the movements of individual cars over time, even when the driver

has not broken any law.[1] Such a database enables agencies, including law enforcement, to undertake widespread, systematic surveillance on a level that was never possible before. These surveillance concerns are exacerbated by long data retention periods because aggregate data becomes increasingly invasive and revealing when it is stored for long periods of time (as acknowledged by the U.S. Supreme Court in the *Carpenter* decision[2]). However, existing law in Seattle places no specific limits on the use of ALPR technology or data, meaning an agency can choose whether and how they want to retain data and track vehicle movements.

Currently, the use of ALPR technology in Seattle chills constitutionally protected activities because they can be used to target drivers who visit sensitive places such as centers of religious worship, protests, union halls, immigration clinics, or health centers. Whole communities can be targeted based on their religious, ethnic, or associational makeup, which is exactly what has happened in the United States and abroad. In New York City, police officers drove unmarked vehicles equipped with license plate readers near local mosques as part of a massive program of suspicionless surveillance of the Muslim community.[3] In the U.K., law enforcement agents installed over 200 cameras and license plate readers to target a predominantly Muslim community suburbs of Birmingham.[4] ALPR data obtained from the Oakland Police Department showed that police disproportionately deployed ALPR-mounted vehicles in low-income communities and communities of color.[5] And the federal Immigration and Customs Enforcement (ICE) agency has sought access to ALPR data in order to target immigrants for deportation.[6]

The foregoing concerns suggest the Council should ensure strong protections in ordinance against the misuse of this technology, regardless of which agency is deploying it and for what purpose.

## Specific Comments and Recommendations

### 1. Automated License Plate Recognition (ALPR) (Patrol) (SPD)

The initial October 2018 Surveillance Impact Report (SIR) for this technology did not indicate the existence of clear policies imposing meaningful restrictions on the purposes for which ALPR data may be collected or used. The updated January 2019 SIR adds a November 2018 memo from SPD Deputy Chief Marc Garth Green (page 42), which states that SPD anticipates having an updated policy by January 31, 2019. The memo states:

> "**New policies:** SPD recognizes that its current ALPR policy needs updating and anticipates that an updated ALPR policy will be in place by January 31, 2019. In addition, SPD has recently updated its policy related to Foreign Nationals, emphasizing that SPD has no role in immigration enforcement and will not inquire about any person's immigration status. In addition, SPD welcomes the OIG to audit its use of ALPR technologies and data."

[1] https://www.eff.org/deeplinks/2013/05/alpr
[2] https://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-Scholars-of-Criminal-Procedure-and-Privacy.pdf
[3] https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques
[4] https://www.theguardian.com/uk/2010/jun/04/surveillance-cameras-birmingham-muslims
[5] https://www.eff.org/pages/automated-license-plate-readers-alpr
[6] https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data

Although the updated SIR (with the November 2018 memo addition) was conveyed to CSWG in March 2019, the SIR does not indicate whether or not the new policies mentioned in the November 2018 memo have already been adopted by SPD, nor include those policies.

Additional concerns regarding this technology are listed below. To address these concerns, we recommend that the Council ensure not only that the minimum rules listed above in the Executive Summary apply to ALPR-Patrol Systems by ordinance, but that the issues noted below with SPD's current policies are addressed as set forth in the corresponding recommendations, all of which should be incorporated into the Council's approval of the technology.

SPD's policy:

- Does not impose meaningful restrictions on the purposes for which ALPR data may be collected or used.
    - *Recommendation: SPD's policy must clearly define and meaningfully restrict the purposes for which ALPR data may be collected, accessed, and used. These purposes should be limited to checking vehicles against specified hotlists connected to specific criminal investigations. SPD must have reasonable suspicion that a crime has occurred (in the context of a specifically defined criminal investigation) before examining collected license plate reader data; they must not examine license plate reader data in order to generate reasonable suspicion. While SPD's ALPR policy says there must be a specific criminal investigation in order for ALPR data to be accessed, it does not describe how such an investigation is defined or documented.*
- Does not justify SPD's 90-day retention period. SPD retains ALPR data for 90 days, but examples given in the SIR of crimes solved using ALPRs largely appear to involve immediate matches against a hotlist. We acknowledge that state law and technical considerations may impact this retention period.
    - *Recommendation: SPD's policy must require a shorter retention period of 48 hours at most, during which time it must use the data for the specified purpose, then immediately delete the data. SPD should retain no information at all when a passing vehicle does not match a hot list (particularly given that such data is subject to public disclosure, including to federal agencies).*
- Does not limit data sharing by policy or statute. The sharing of ALPR data with other agencies is of great concern, and SPD states a variety of situations in which such data may be shared (see SIR Section 6.1). However, the policies cited do not make clear the criteria for such sharing, nor any inter-agency agreement that governs such sharing, nor why the data must be shared in the first place. The November 2018 memo only adds the statement, "SPD limits data-sharing with other law enforcement agencies for official law enforcement purposes," which does not address the concerns above.
    - *Recommendation: SPD's policy must limit sharing of ALPR data to third parties that have a written agreement holding those third parties to the same use, retention, and access rules as SPD; make clear to whom and under what circumstances the data are disclosed; and make publicly available a list of what disclosures have been made to which third parties.*

- Does not make clear whether and how audits of inquires to the system can be conducted (see SIR Sections 4.10 and 8.2, for example). The November 2018 memo does not add any new information.
    - *Recommendation: SPD's policy must include a regular audit system to protect against abuse.*
- Does not make clear how and to what degree Patrol and Parking Enforcement ALPR systems are separated, and whether SPD's policies on ALPR apply to the Parking Enforcement Systems (whose data may be equally prone to misuse).
    - *Recommendation: SPD's policy must include strong protections against abuse that are applied to all ALPR systems.*
- Does not include measures to minimize false matches.
    - *Recommendation: SPD's policy must specific that whenever a hit occurs, an officer, before taking any action, must confirm visually that a plate matches the number and state identified in the alert, confirm that the alert is still active by calling dispatch and, if the alert pertains to the registrant of the car and not the car itself, for example in a warrant situation, develop a reasonable belief that the vehicle's occupant(*s*) match any individual(s) identified in the alert.*
- Does not include systematic tracking to assess how many crimes each year are actually solved using ALPR data.
    - *Recommendation: SPD's policy must require detailed records of ALPR scans, hits, and crimes solved specifically attributable to those hits, as well as an accounting of how ALPR use varies by neighborhood and demographic*.
- Does not create clear restrictions on who can access the data.
    - *Recommendation: SPD's policy must require access controls on the ALPR databases, with only agents who have been trained in the policies governing such databases permitted access, and with every instance of access logged.*

**2. Parking Enforcement Systems (Including ALPR) (SPD)**

As with the updated ALPR-Patrol SIR, the January 2019 Parking Enforcement Systems SIR includes a November 2018 memo from SPD Deputy Chief Marc Garth Green (page 39) stating that SPD anticipates having an updated policy by January 31, 2019. Again, although the updated SIR was conveyed to CSWG in March 2019, it does not indicate whether or not these new policies have already been adopted by SPD, nor address issues previously highlighted in public comment.

Particularly given the partly merged nature of the Parking Enforcement and Patrol ALPRs, including use of the Parking Enforcement ALPRs to check vehicle plates against hot lists, the concerns and recommendations stated above with respect to SPD Patrol ALPRs (e.g., data access, clear standards for data sharing with third party entities, clear purpose of sharing, auditing requirements) apply equally to Parking Enforcement Systems. The Council should therefore ensure that the same minimum rules (listed in the Executive Summary) apply to Parking Enforcement Systems via ordinance, and that the issues noted below with SPD's current policies are addressed as set forth in

the corresponding recommendations, all of which should be incorporated into the Council's approval of the technology.

SPD's policy:

- Does not make clear how the Parking Enforcement ALPR systems integrate with the Patrol ALPR systems—it appears that some integration occurs at least in the case of the Scofflaw enforcement vans that store collected data in the BOSS system.
    - *Recommendation: SPD's policy must require that the data collected by Parking Enforcement ALPR systems is not shared with Patrol ALPR systems.*
- Does not make clear whether software and hardware providers (as mentioned in Section 2.3 of the SIR) all contract directly with SPD itself, with each other, or with a third-party entity to provide ALPR and related services.
    - *Recommendation: SPD's policy must require all data-sharing relationships to be disclosed to the public in clear terms, and, as stated above in the ALPR-Patrol Section, SPD's policy must limit sharing of ALPR data to third parties that have a written agreement holding those third parties to the same use, retention, and access rules as SPD, and requiring disclosure of to whom and under what circumstances the data are disclosed.*
- Does not include systematic tracking to assess the numbers of scans, hits, and revenue generated from the Parking Enforcement ALPR systems.
    - *Recommendation: SPD's policy must require detailed records of ALPR scans, hits, and revenue generated specifically attributable to those hits, as well as an accounting of how ALPR use varies by neighborhood and demographic*.
- Does not make clear whether pictures of the vehicle are being taken in addition to the license plate, and if so, if and for how long these pictures are stored (Section 4.1)
    - *Recommendation: SPD's policy must make explicit what photos are taken by the ALPR on Parking Enforcement vehicles, and require the same 48-hour maximum retention period for all photos.*

**3. License Plate Readers (LPR) (SDOT)**

In contrast to the SPD SIRs, the License Plate Readers (SDOT) SIR clearly defines and states meaningful restrictions on the purposes for which LPRs data may be collected, accessed, and used; it states that no license plate data is retained by SDOT or WSDOT; and it states that the license plate information SDOT accesses will never be used as a part of any criminal investigation.

However, it remains unclear whether SDOT's stated no-retention practice is reflected in written policy. Furthermore, SDOT's use of LPRs poses the concern of data sharing with a state entity (WSDOT). It is unclear whether an explicit agreement exists between SDOT and WSDOT ensuring that WSDOT uses the data only for the purpose of calculating travel times, and deletes the data immediately after such use.

In addition to the minimum standards stated in the Executive Summary, the Council should in its approval of this technology ensure that:

1. The LPR data collected by SDOT is used only for the purpose of calculating travel times, and explicitly never for criminal or law enforcement purposes.
2. No LPR data is retained.
3. No third party other than SDOT and WSDOT can access the LPR data at any time.
4. A written agreement holds WSDOT to the above restrictions.