Shankar Narayan
TECHNOLOGY AND LIBERTY PROJECT DIRECTOR

October 24th, 2018

RE: ACLU-WA Comments Regarding Group 1 Surveillance Technologies

Dear Seattle IT:

On behalf of the ACLU of Washington, I write to offer the ACLU-WA's comments on the surveillance technologies included in Group 1 of the Seattle Surveillance Ordinance process. We are submitting these comments by mail because they do not conform to the specific format of the online comment form provided on the CTO's website, and because the technologies form groups in which some comments apply to multiple technologies.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON
901 5TH AVENUE, STE 630
SEATTLE, WA 98164
T/206.624.2184
WWW.ACLU-WA.ORG

JEAN ROBINSON
BOARD PRESIDENT

KATHLEEN TAYLOR
EXECUTIVE DIRECTOR

These comments should be considered preliminary, given that the Surveillance Impact Reports for each technology leave a number of significant questions unanswered. Specific unanswered questions for each technology are noted in the comments relating to that technology, and it is our hope that those questions will be answered in the updated SIR provided to the City Council prior to its review of that technology.

The technologies in Group 1 are covered in the following order:

I. Automated License Plate Recognition (ALPR) Group

1. Automated License Plate Recognition (ALPR)(Patrol)(SPD)
2. Parking Enforcement Systems (Including ALPR)(SPD)
3. License Plate Readers (SDOT)

II. Camera Group

1. Emergency Scene Cameras (SFD)
2. Hazardous Materials (Hazmat) Camera (SFD)
3. Closed Circuit Television "Traffic Cameras" (SDOT)

I. ALPR Group

Automated License Plate Reader Systems (ALPRs) are powerful surveillance technologies that have the potential to 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 community members doing nothing more than going about their daily business. Indeed, at the first public meeting seeking comment on the SPD Patrol ALPRs, it was revealed that the ALPR system collected

37,000 license plates in a 24 hour period—which equates to over *13.5 million* scans over a full year. The overwhelming majority of these drivers are not suspected of any crime.

With this massive database of information, agencies can comprehensively track and plot the movements of individual cars over time, even when the driver has not broken any law. This enables agencies, including law enforcement, to undertake widespread, systematic surveillance on a level that was never possible before. Aggregate data stored for long periods of time becomes more invasive and revealing. 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.

ALPR technology 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, and indeed, exactly that has happened elsewhere. In New York City, police officers drove unmarked vehicles equipped with license plate readers around local mosques in order to record each attendee as part of a massive program of suspicionless surveillance of the Muslim community. In the U.K., law enforcement agents installed over 200 cameras and license plate readers to target a predominantly Muslim community suburbs of Birmingham. ALPR data obtained from the Oakland Police Department showed that police there disproportionately deployed ALPR-mounted vehicles in low-income communities and communities of color. And the federal Immigration and Customs Enforcement agency has sought access to ALPR data in order to target immigrants for deportation. All of these concerns are magnified in light of a long history of the use of invasive surveillance technologies to target vulnerable communities (see, for example, Simone Browne's excellent, multidisciplinary book on the subject, *Dark Matters: On the Surveillance of Blackness*).

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

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

The SIR relating to Patrol ALPRs raises a number of specific concerns around current policy and practice, and leaves open a number of significant questions. I attempt to capture these in sections below on concerns, questions, and recommendations.

a. Major Concerns

- *Inadequate Policies.* Policies cited in the SIR are vague, contradictory, and appear to impose no meaningful restrictions on the purposes for which ALPR data may be collected or used. Policy 16.170—the only apparent policy specific to ALPRs—for example, is very short, contains undefined terms, and focuses on training rather than use. Subsection 3 of the policy says that "ALPR Operation Shall be for Official Department Purposes" and that ALPR may be used "during routine patrol or any criminal investigation." This does not meaningfully restrict

the purposes for which ALPR may be used. And another part of the policy states that ALPR data may be accessed only when it relates to a specific criminal investigation—yet it is unclear how this relates to the enforcement of civil violations mentioned in both SPD SIRs. More generally, much of the practice described in the SIR does not appear to be reflected in any written policy at all (for example, the practice of manually verifying a hit visually is not reflected in policy).

- *Dragnet Use with No Justification*. While the SIR contains contradictory information on this point, it appears that ALPR cameras are always running, offering a vast dragnet of data collection. No legal standard is stated to justify this general, dragnet use. The Seattle Intelligence Ordinance is cited, but SPD seems to assume that dragnet surveillance is consistent with this Ordinance, without any specific policy (for example, are ALPR-equipped vehicles kept away from protests?).

- *Lengthy Retention Window with No Justification*. 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. It is unclear what justifies this long retention window.

- *Data Sharing is Not Explicitly Limited 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). But 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 (see perfunctory answer to SIR Section 6.2). This issue of data sharing was raised in the enactment of the Surveillance Ordinance itself, and has only become more urgent under the current federal administration.

- *Inadequate Auditing*. The SIR appears to contradict itself on the subject of whether and how audits of inquiries to the system can be conducted (see SIR Sections 4.10 and 8.2, for example). As with any invasive surveillance system, a clear and regular audit trail to protect against abuse is important.

b. *Outstanding Questions*

I'm listing questions here that I hope will be answered in an updated SIR:

- To what degree are patrol and parking enforcement ALPR systems are separated, and do SPD policies on ALPR apply fully to the Parking Enforcement Systems? It appears the systems are merged at least to some extent, and in that case, the same strong protections against abuse should be applied to all systems.

- ALPR policy says there has to be a specific criminal investigation in order for ALPR data to be accessed. Does reasonable suspicion of a crime equate to a

specific criminal investigation? How is a specific criminal investigation documented?

- Under what agreements is data shared with outside agencies, and where "required by law," what specific laws require this sharing? To which systems outside SPD is data uploaded?

- How many plate images collected by the system every day? What is the hit rate on those images? Is there systematic data reflecting how many crimes each year are actually solved using ALPR data?

- How often do misreads occur? Are they systematically tracked?

c. *Recommendations*

These recommendations should be considered preliminary, pending answers to the questions above. But we urge the Council to ensure binding enforceable protections in ordinance that ensure the following minimum protections:

- Dragnet use and long retention of ALPR data should be outlawed. SPD must have reasonable suspicion that a crime has occurred before examining collected license plate reader data; they must not examine license plate reader data in order to generate reasonable suspicion. 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).

- People should be able to find out if plate data of vehicles registered to them are contained in SPD's ALPR database. They should also be able to access the data.

- There must be 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.

- SPD should not share any ALPR data with third parties without a written agreement ensuring that those third parties conform to the above retention and access rules, and should disclose to whom and under what circumstances the data are disclosed.

- 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.

- ALPRs should not be used for non-criminal enforcement purposes, other than parking enforcement.

- SPD should produce 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.

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

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 stated above with respect to SPD Patrol ALPRs apply equally to parking enforcement systems, and Council should ensure that the same minimum rules apply to them via ordinance—the intended primary use for parking enforcement does not in itself mitigate the concerns raised. In addition, the following outstanding questions should be answered in an updated SIR:

- It is unclear from the SIR 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. An updated ALPR should clarify specifically what rules apply to that data, and how they differ from rules applied to data collected by Patrol ALPR.

- A number of software and hardware providers are mentioned in Section 2.3 of the SIR—an updated SIR should clarify whether all contract directly with SPD itself, or with each other or a third party entity, to provide ALPR and related services.

- As with Patrol ALPR, statistics on numbers of scans, hits, and revenue from the systems would be helpful.

- Section 4.1 suggests pictures of the vehicle are being taken in addition to the plate—are these pictures stored, and if so, for how long?

- Concerns set forth in the section above relating to patrol ALPR regarding data access, clear standards for data sharing with third party entities and the purpose of such sharing, as well as auditing, all apply to these systems as well—and an updated SIR should clarify those standards.

3. License Plate Readers (SDOT)

The concerns stated above with respect to patrol ALPR largely apply to this set of ALPRs as well, with the additional concern of explicit sharing with a state entity. It is heartening that the SIR suggests that no license plate data is retained, but it is not clear whether that no-retention practice is reflected in policy. It is also unclear whether an explicit agreement exists with WSDOT ensuring deletion of the data and use only for the

purpose of calculating travel times. With that in mind, the following outstanding questions should be answered in an updated SIR:

- What explicit, written policies govern what SDOT and WSDOT can do with this ALPR data? Is there a written agreement with WSDOT requiring no personal data collection and deletion of all data?

- Under what circumstances might this data be used for law enforcement purposes? Is it possible for third parties to subpoena any data retained?

- What additional third parties get access to the data?

The Council should ensure by ordinance that the data collected is used only for the purpose of calculating travel times, that no data is retained, that no third party other than SDOT and WSDOT access the data at any time, and that a written agreement holds WSDOT to these restrictions.

II. Camera Group

Overall, concerns around this group of technologies largely focus on the use of these systems and the data collected by them for purposes other than those intended, over-collection and over-retention of data, and sharing of that data with third parties (such as federal law enforcement agencies). While the stated purposes of the cameras may be relatively innocuous, it is important to remember that images taken by such cameras, for example at emergency scenes, can compromise the privacy of individuals at vulnerable moments, and can be misused for the same kinds of targeting and profiling of particular communities detailed in Section I above. In addition, with the widespread and cheap availability of facial recognition technology, which can be applied after the fact to any image showing a face, it is all the more important that protections limiting the use of these tools to their intended purpose be enacted.

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

- The purpose of camera use should be clearly defined, and its operation and data collected should be explicitly restricted to that purpose only.

- Data retention should be limited to the time needed to effectuate the purpose defined.

- Data sharing with third parties should be limited to those held to the same restrictions.

- Clear policies should govern operation, and all operators of the cameras should be trained in those policies.

Specific comments follow:

1. Emergency Scene Cameras (ESCs)(SFD)

The SIR for this technology states that no explicit internal policy exists at SFD that governs the use of ESCs, so a good start would be to create such a policy and include it in an updated SIR. This process should begin with an explicit list of specific uses for the ESCs, which are currently only set forth in general terms, and with apparent contradictions between sections of the SIR (for example, Section 1.0 describes three uses for the cameras, but Section 2.1 adds several more). In addition, the updated SIR should set forth any other internal internal policies and Washington laws governing use, retention, and disclosure of the data; where the data is stored; and which third parties, if any, have access to it, and for what purpose. (The SIR indicates data sharing with SPD, but the purpose is not clear.)

In turn, the Council should ensure via ordinance that no use is made of the images beyond the specific emergency, investigative, or training uses set forth, and that the data is deleted immediately upon completion of those purposes. Data sharing with third parties should be prohibited unless for those specific uses, and those third parties should be held to the same use and retention standards.

2. Hazardous Materials (Hazmat) Cameras (SFD)

As with ESCs, the SIR for Hazmat cameras indicates that no policy governing the use of this technology currently exists, with one limited exception for mechanism-of-injury recordings (see SIR Section 3.3). So similarly to ESCs, with this technology, an explicit policy that lists specific uses for the cameras should be created and included in an updated SIR. In addition, answers to questions such as who stores the data and which third parties have access to it should be made explicit. In particular, the SIR describes data sharing with law enforcement, but purposes of that disclosure are not made explicit (see SIR Section 4.7). In instances where a legal standard such as reasonable suspicion is applied, it should be clear what the standard is, who applies it, and how that application is documented. Overall, use of this technology should be limited to emergency response purposes, and any law enforcement use of the data should be restricted by ordinance.

3. Closed Circuit Television "Traffic Cameras" (SDOT)

As with the other two camera technologies, the crux of concern around these traffic cameras relates to limiting their use to specific purposes, enshrining in statute protections against invasion of privacy and general data collection, and limiting data sharing. It would be helpful to see the SDOT camera control guidelines referenced in the SIR, as well as to make clear in a policy applicable specifically to these cameras, what data will be deleted when (Section 5 appears to contain several different retention policies). Additional questions that an updated SIR should answer are as follows:

- The current SIR does not reference specific camera vendors and models—these would be helpful to have.

- Are there currently explicit guidelines on when recording occurs, and what's maintained? (See SIR Section 3.3 referencing recording for "compelling traffic operational needs"—the term is undefined.)

- Law enforcement use appears to be explicitly contemplated by the SIR, but the specific allowable uses are not defined—these should be made clear.

As with the other camera technologies, the Council should ensure clear purposes are defined in statute for these traffic cameras, that no use is made of the images for other purposes, that data is immediately deleted when the purpose is achieved, and that data sharing with third parties should be prohibited unless for those specific uses.

Thank you for your consideration, and we look forward to working with you on the process of ordinance implementation. Please feel free to contact me with questions or concerns.

Sincerely,

Shankar Narayan

cc: Seattle City Council and Executive