PRIVACY AND CIVIL LIBERTIES IMPACT ASSESSMENT

The Surveillance Advisory Working Group's Privacy and Civil Liberties Impact Assessment (PCLIA) for Seattle Department of Transportation's (SDOT) License Plate Readers (LPR) technology is below.

Please note, the Working Group's PCLIA for SDOT's LPR was part of larger report which included reviews of additional retroactive surveillance technologies not applicable to this Council submission. As such, the Working Group's assessment for these additional technologies has been removed from this report, and will be made available in the appropriate SIRs, to be submitted to Council at a later date.

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

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.

---

[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