

Surveillance Usage Review: Seattle Department of Transportation License Plate Readers

December 30, 2020

Megumi Sumitani

David G. Jones, City Auditor



Seattle Office of City Auditor

Surveillance Usage Review: Seattle Department of Transportation License Plate Readers

Report Highlights

Background

The Seattle Department of Transportation's (SDOT's) License Plate Readers (LPR) technology is used for capturing license plate information to calculate the average travel time between two locations on Seattle's streets. LPR cameras are high definition cameras specifically designed to capture images of license plates as they move into view. The LPR data are processed by software that reports the license plate number to the Washington State Department of Transportation (WSDOT), and WSDOT processes the travel time between the two locations and sends the travel time information back to SDOT. SDOT posts the travel time information to the public on its roadside signs and on its [Traveler Information Web Map](#) for the public to use in making informed trip decisions.

What We Found

Contrary to the requirement outlined in the legislation governing LPR passed by the City Council, there is no written agreement between SDOT and WSDOT regarding WSDOT's sharing, retention, and deletion of SDOT's LPR data. This includes what WSDOT can or cannot do with LPR data outside of its agreement with SDOT. The absence of a written agreement increases the risk that SDOT's LPR data will not be used appropriately by WSDOT. SDOT officials told us that they have had numerous conversations with WSDOT, and that creating an agreement would require an SDOT funded investment to support WSDOT's multi-departmental review team. Consequently, SDOT decided not to continue to allocate resources to support the LPR technology, which is aging and nearing the end of its service life, and instead replace LPR technology with Acylica sensors to provide travel time information. SDOT reported that it will complete the replacement of the LPR system with Acylica technology by the end of 2021.

Additional work will be required to ensure information assurance for LPR data, which could, through malicious attack or other inadvertent or improper sharing, affect an individual's civil liberties.



WHY WE DID THIS AUDIT

This audit is required by: Ordinance 125376, which requires the City Auditor to conduct an annual review of the City's use of City Council-approved non-police surveillance technologies, and Ordinance 125936, which approved the use of SDOT's LPR technology.

HOW WE DID THIS AUDIT

To accomplish the audit's objectives, we:

- Reviewed the 2018 Surveillance Impact Report (SIR) and 2019 Condensed Surveillance Impact Report (CSIR), attachments to Ordinance 125936,
- Interviewed SDOT officials who manage and operate LPR technology,
- Analyzed data pertaining to complaints and concerns about LPR technology and demographic information of LPR camera locations, and
- Obtained cost data for the use of LPR technology.

Seattle Office of City Auditor

David G. Jones, City Auditor
www.seattle.gov/cityauditor

Recommendations

We make nine recommendations in our report, including that SDOT should execute a written agreement with WSDOT about the use of LPR data and engage cybersecurity experts to conduct regular security assessments. We also recommend that applicable SIR and CSIR operational policies be revised so that they are consistent with how WSDOT deletes the data it receives from SDOT; that technical testing be conducted by cybersecurity experts to verify compliance with several operational policies; that operational policy discrepancies between the SIR and CSIR be resolved; and that required training on the handling and use of LPR data be documented.

Department Response

In their formal, written response to our report SDOT stated that they concurred with the report's findings and recommendations. Please see Appendix A for SDOT's response to our findings.

TABLE OF CONTENTS

INTRODUCTION	1
A. SURVEILLANCE TECHNOLOGY USE AND TRENDS	4
Compliance Summary: Surveillance Technology Use and Trends	6
B. TECHNOLOGY AND DATA SHARING	7
Compliance Summary: Technology and Data Sharing	11
C. PROTOCOLS FOR DATA MANAGEMENT	15
Compliance Summary: Protocols for Data Management	20
D. CIVIL LIBERTIES IMPACT	23
Compliance Summary: Civil Liberties Impact	27
E. COMPLAINTS, CONCERNS, AND OTHER ASSESSMENTS	28
F. COSTS	30
OBJECTIVES, SCOPE, AND METHODOLOGY	32
APPENDIX A	34
Department Response	34
APPENDIX B	36
List of Recommendations	36
APPENDIX C	39
Operational Policies Cross-Referencing Matrix	39
APPENDIX D	43
Operational Policies Compliance Matrix (consolidated for all report sections)	43
APPENDIX E	45
License Plate Readers (LPR) Technology	45
APPENDIX F	48
SDOT-WSDOT Data Sharing (How SDOT Shares LPR Data with WSDOT)	48
APPENDIX G	50
Population Density	50
APPENDIX H	51
Race and Social Equity Composite Index	51
APPENDIX I	52
Acknowledgements	52
APPENDIX J	53
Seattle Office of City Auditor Mission, Background, and Quality Assurance	53

INTRODUCTION

Audit Overview

This audit on the Seattle Department of Transportation's (SDOT) use of License Plate Readers (LPR) technology is required by Seattle Municipal Code 14.18.060 (Ordinance 125376 "Acquisition and Use of Surveillance Technologies"), which requires the City Auditor to conduct an annual review of the City's use of surveillance technologies used by all City departments except the Seattle Police Department and the extent to which departments are in compliance with the requirements of Chapter 14.18 and the terms of approved Surveillance Impact Reports (SIRs).

The ordinance states that the review should include, but not be limited to the following:

- A. How surveillance technology has been used, how frequently, and whether usage patterns are changing over time;
- B. How often surveillance technology or its data are being shared with other entities, including other governments in particular;
- C. How well data management protocols are safeguarding individual information;
- D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated;¹
- E. A summary of any complaints or concerns received by or known by departments about their surveillance technology, and the results of any internal audits or other assessments of code compliance; and
- F. Total annual costs for the use of surveillance technology, including personnel and other ongoing costs.

In their response to our report, the Seattle Department of Transportation stated that they concurred with our findings and recommendations.

¹ In its entirety, Ordinance 125376, Section 14.18.060, D states: How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated, including, for SPD, an examination of whether deployments are pursuant to warrants or not and how SPD's surveillance technology is used to analyze patterns to predict suspect, individual, or group-affiliation behavior. Here, we omitted the reference to SPD (the Seattle Police Department) because this technology is not an SPD technology. The Inspector General for Public Safety is responsible for the annual surveillance usage review for SPD technologies.

We thank individuals from City of Seattle departments, the Washington State Department of Transportation (WSDOT), and other outside entities for their cooperation and assistance. They are listed in Appendix I. The audit team for this project included Melissa Alderson and Megumi Sumitani.

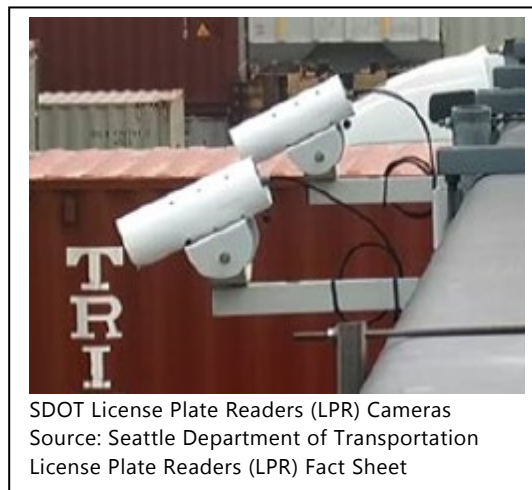
Legislative Background

SDOT’s license plate readers (LPR) technology is a legacy technology that predates the Seattle’s “Surveillance Ordinance” (Ordinance 125376) passed in July 2017. The Surveillance Ordinance is intended to provide greater transparency to the City Council and the public when a City of Seattle (City) department acquires or uses surveillance technology that raises concerns about privacy or other civil liberties, and involves new and legacy technologies that require City Council review and approval for their use. The City Council approved the use of SDOT’s LPR technology as a surveillance technology via Ordinance 125936 in September 2019.

What criteria did the Office of City Auditor use in this review?

We used the operational policy statements in the LPR Surveillance Impact Report (SIR) and LPR Condensed Surveillance Impact Report (CSIR) as the criteria to assess the evidence we gathered (e.g., from interviews) about whether the technology was being used in accordance with legislative requirements. Please refer to Appendix C.

What is License Plate Readers technology?



LPR technology is a combination of hardware and software used for capturing and monitoring images of license plates. LPR cameras are installed on dedicated mast arms that are connected to signal poles and positioned over travel lanes at various intersections throughout Seattle. Electrical power

is provided from the nearest traffic signal cabinet.

SDOT’s LPR technology is primarily used for determining travel times by automobiles between certain points on Seattle’s streets. SDOT shares this information with the public by roadside electronic signs and through the [Traveler Information Web Map](#) so that individuals

can make informed trip decisions. SDOT also uses the travel times for its own system engineering² and traffic planning³ purposes.

SDOT acquired the technology in 2011 through a federal grant and deployed it in 2012. SDOT's LPR technology is part of the City of Seattle's Intelligent Transportation System (ITS),⁴ which uses electronics and communications technologies to enhance mobility for all transportation modes by increasing the efficiency and safety of the transportation infrastructure.⁵

Please see Appendix E for more detailed information about LPR technology.

How long does SDOT plan to use its License Plate Readers Technology for traffic information purposes?

According to SDOT, no new LPR cameras have been acquired since about 2010 and SDOT does not plan to acquire any new LPR cameras for calculating travel times. While SDOT will maintain or repair an LPR camera, if one needs to be replaced, it will be replaced with Acyclica technology. Acyclica technology is in Group Two of the Master List of Surveillance Technologies, and as of this report, its SIR is scheduled for review and approval by City Council in late 2020 or early 2021.

The physical location for the management of the City's Intelligent Transportation System (ITS) infrastructure is SDOT's Transportation Operations Center (TOC), located on the 37th floor of the Seattle Municipal Tower. The TOC monitors congestion and traffic incidents; operates traffic cameras, dynamic message signs; and posts travel times to the public. SDOT officials told us that due to the age of the devices, SDOT's LPR cameras are failing with increasing frequency, are at "end-of-life," and no longer supported by the manufacturer. As a result, SDOT began a program to replace irreparable LPR cameras with Acyclica sensors to provide travel time information. SDOT told us that they will complete the replacement of the LPR system by the end of 2021.

² System engineering in this context is evaluating and applying travel time data to determine solutions to make the streets work better, i.e., improving traffic flow for particular transportation modes such as busses and bicycles.

³ An example of traffic planning would be studying the effectiveness of an operational change such as signal timing adjustments.

⁴ ITS core investments and infrastructure include: traffic signal controllers, cabinets, detection and displays; the citywide ITS communications network; traffic cameras that enable staff to view operations and dynamically adjust traffic signal timing if needed; Dynamic Message Signs (DMS) that provide on-street traveler information; the traveler's website (www.seattle.gov/travelers) that includes congestion information, traffic advisories and traffic camera images; the Traffic Operations Center (TOC) that includes processing, monitoring, and communications equipment allowing staff to interact with the systems; and the staff that operate and maintain these assets. Source: [ITS Strategic Plan](#), p. 1

⁵ [ITS Strategic Plan](#), Overview, p. 1

A. SURVEILLANCE TECHNOLOGY USE AND TRENDS

Section Summary

To understand how surveillance technology is being used, how frequently, and whether usage patterns have changed over time,⁶ we interviewed knowledgeable SDOT officials who manage and operate SDOT's License Plate Readers (LPR) technology and visited SDOT's Transportation Operations Center (TOC) in the Seattle Municipal Tower. We found that LPR are used for several purposes, including system engineering and traffic planning, but primarily for providing travel times to the public for use in making trip decisions. The technology is not used for any enforcement purposes. LPR cameras are continuously in operation, collecting data and transmitting information to the Washington State Department of Transportation (WSDOT) 24 hours, every day of the year. We were not able to report on whether usage patterns have changed over time because data showing usage or consumption of the LPR information does not exist.

How does SDOT use travel time information?

SDOT officials reported that they use the travel time information from LPR for system engineering, traffic planning, and public distribution purposes. This is consistent with **Operational Policy 1**. They explained that SDOT evaluates and applies travel time data to determine solutions to make the streets work better, such as improving traffic flow for transportation modes like busses and bicycles. SDOT also uses the travel time information to study the effectiveness of an operational change such as signal timing adjustments. As for public distribution, SDOT posts travel times to SDOT Dynamic Message Signs (DMS)⁷ and on SDOT's [Traveler Information Map](#) web application. The SDOT TOC Manager told us that public distribution of travel times comprises over 95 percent of LPR activities in the TOC.

⁶ Ordinance Question A: How surveillance technology has been used, how frequently, and whether usage patterns are changing over time.

⁷ "DMS are the large, electronic signs which overhang or appear along major streets throughout Seattle. The signs are typically used to display information about traffic conditions travel times, construction, and road incidents. Travel time information is the default message that appears on a DMS daily from 5AM-9AM, and 4PM-7PM along 12 corridors. With this type of information displayed, drivers can make real time route choices given the traffic conditions ahead. Recently, SDOT has begun to combine the LPR travel time data with SDOT's other travel time technology (Acyclica) to provide information to even more destinations. SDOT also provides travel time information on the [Traveler Information Map](#) web application." (Traffic Cameras SIR 2.3)

Does SDOT use travel time information for enforcement purposes?

We asked SDOT about the reference in **Operational Policy 10** to “work zone congestion enforcement.” The SDOT TOC Manager told us that they do not use travel time information for any enforcement purposes; instead, the term refers to when SDOT uses travel time information to understand how streets or corridor travel times are being affected by things happening in them, for example, non-City construction work (work zones) that affect streets or corridors.

To ensure that Operational Policy 10 is consistent with SDOT’s practice and to help assure the public that SDOT’s LPR system is not being used for enforcement purposes, SDOT should update Operational Policy 10 to state that the LPR system is built for and to be used for only for traffic management and optimization purposes, and *not for any enforcement purposes*.

Recommendation 1

The Seattle Department of Transportation should remove the word “enforcement” from Surveillance Impact Report Operational Policy 10 and Condensed Surveillance Impact Report Operational Policy 5.0, 4, and revise the references to this work to clarify that it refers to work zone congestion analysis and not enforcement.

How frequently are License Plate Readers technologies used?

LPR technology collects data 24 hours a day, seven days a week, 365 days a year. LPR cameras are powered on and functioning all the time, and automatically transmit their data to WSDOT for processing without any user intervention.

How has the use of License Plate Readers information changed over time?

We could not answer this question because data showing usage of the LPR information does not exist. According to SDOT, there are no data available on LPR usage or consumption of LPR travel time information. LPR technology and LPR cameras are continually operating and LPR data is automatically transmitted by SDOT to WSDOT for processing and WSDOT’s system automatically transmits processed travel times to SDOT without any user intervention.

Compliance Summary: Surveillance Technology Use and Trends

Is SDOT in compliance with the relevant operational policies related to surveillance technology use?

Based on the evidence we reviewed, SDOT appears to be in compliance with both operational policies relevant to use of this surveillance technology. However, one of the policies needs to be corrected so that it is consistent with SDOT’s practice.

There are two operational policies relevant to the use of this surveillance technology: Operational Policy 1 and Operational Policy 10. See details in Exhibit 1 below.

Exhibit 1: Operational Policies Compliance Matrix LPR Use

Operational Policy	Is SDOT in compliance?	Recommendation(s)/ Comments
<p>Operational Policy 1: The SDOT LPR System and the travel time information produced by it is used only for system engineering, traffic planning, and public distribution purposes. [Same as CSIR Operational Policy 1.0, 1]</p>	<p>YES</p>	
<p>Operational Policy 10: Applications of travel time information in the Department include: signal timing and coordination, traffic network optimization, street parking, congestion analysis, congestion mapping, route planning, work zone congestion enforcement, variable message signs, incident detection, emergency responder routing and route utilization. [Same as CSIR Operational Policy 5.0, 4]</p>	<p>YES</p>	<p>We assessed that SDOT is not out of compliance with the Operational Policy but that the wording of the policy needs to be corrected to be consistent with SDOT’s practice.</p> <p>Recommendation 1: The Seattle Department of Transportation should remove the word “enforcement” from Surveillance Impact Report Operational Policy 10 and Condensed Surveillance Impact Report Operational Policy 5.0, 4, and revise the references to this work to clarify that it refers to work zone congestion analysis and not enforcement.</p>

B. TECHNOLOGY AND DATA SHARING

Section Summary

To understand how surveillance technology and data are being shared with other entities,⁸ we interviewed SDOT Transportation Operations Center officials who manage and operate SDOT's LPR technology, and communicated with Washington State Department of Transportation (WSDOT) [Intelligent Transportation Systems Operations](#) officials concerning the collection, processing, retention, and deletion of LPR data. We found that SDOT shares its LPR data with WSDOT. WSDOT processes the data and provides travel times for SDOT. SDOT posts this information for Seattle travelers to use in making trip decisions. Although an SDOT operational policy requires it, there is no written data sharing agreement between SDOT and WSDOT. A data sharing agreement should define how the LPR data is protected, used, and shared. Due to resource constraints which prevented us from contracting with IT security consultants, we were not able to determine whether SDOT is limiting access, storing, or using the LPR data for anything other than for traffic management purposes.

Why does SDOT share License Plate Readers data with WSDOT?

The LPR Surveillance Impact Report (SIR) states that data sharing with the Washington State Department of Transportation (WSDOT) is necessary because WSDOT processes the LPR data and provides SDOT travel times based on that information. SDOT and WSDOT have established an intergovernmental data network for the data exchange.

Does SDOT have a written License Plate Readers data sharing agreement with WSDOT?

No. Although **Operational Policy 14** requires a written data sharing agreement between WSDOT and SDOT, no such agreement is in place. A WSDOT official stated that WSDOT is simply donating some computer time to process SDOT's data and that it was easier and cheaper to process the license plate records data into travel times for SDOT than to try to assist SDOT with writing their own program to calculate travel times. SDOT also confirmed that because WSDOT had a system set up for processing travel time data, it made sense for SDOT to use WSDOT's system rather than SDOT starting from scratch to develop their own system.

⁸ Ordinance Question B: How often surveillance technology or its data are being shared with other entities, including other governments in particular.

The absence of a written agreement increases the risk that SDOT's LPR data will not be used appropriately by WSDOT.

According to the [University of Chicago University Research Administration](#) regarding data sharing agreements, a written agreement of this type should, at a minimum, cover data sharing, retention, and deletion of LPR data, including what WSDOT can and cannot do with LPR data. Although SDOT told us that they are developing a written agreement, a written agreement is still not in place.

Recommendation 2

The Seattle Department of Transportation should execute a written agreement with the Washington State Department of Transportation that, at a minimum, addresses data sharing, retention, and deletion of License Plate Readers data, including what the Washington State Department of Transportation can and cannot do with License Plate Readers data outside of its agreement with the Seattle Department of Transportation.

Is WSDOT sharing the data provided by SDOT with any other entities?

WSDOT officials told us that WSDOT has never shared information from SDOT and could not provide such information, even if requested. We asked WSDOT officials if they share, have shared, or have been asked to share SDOT LPR data with anyone outside WSDOT, such as federal, state, or local law enforcement agencies. WSDOT told us that no one has asked them for the license plate data, and that they could not provide such data even if requested because they only hold temporary reads which are not disclosable.

How does SDOT share License Plate Readers data with WSDOT?

SDOT shares LPR data with WSDOT via a secure fiber-optic network, and the data is not encrypted as there is a dedicated, secure fiber optic network between SDOT and WSDOT. Details of how these data are shared and a data flow diagram is provided in Appendix F.

How often are License Plate Readers data shared with WSDOT?

SDOT's LPR data are shared continuously with WSDOT because LPR technology collects data 24 hours a day, seven days a week, 365 days a year. LPR cameras are powered on and functioning all the time. The devices automatically transmit their data to WSDOT for processing without any user intervention.

What data are being shared with WSDOT?

SDOT's LPR cameras capture images of license plates as they move into a camera's view, and the raw data for each capture, which include a time stamp and the license plate's alphanumeric string, are transmitted to WSDOT. An SDOT engineer told us that no photos of license plates are transmitted. **Operational Policy 3** requires that each data record will be comprised of: time stamp, station identifier, camera channel, alphanumeric plate string, and confidence factor. We confirmed that these elements are being transmitted to WSDOT

by having an SDOT engineer log into an LPR camera and show us these items.

Is the data shared with WSDOT properly deleted?

WSDOT is not deleting the license plate data as stated in **LPR SIR Operational Policy 12** and **CSIR Operational Policy 4.0, 6**. Both policies state that LPR data must be deleted after they are used by WSDOT, but WSDOT officials told us that SDOT's license plate data are converted into identifiers that are anonymized and written to disk in temporary files and held for seven days; all temporary files greater than seven days are automatically purged at 4:00 AM every morning. WSDOT told us they hold the data for seven days in order to pull and use the stored, anonymized data for troubleshooting. For example, to see if their system has any processing errors in calculating travel times. WSDOT told us that they chose the seven-day period.

We asked SDOT if it has evidence that WSDOT is deleting the LPR data after seven days; SDOT told us that they do not. We determined that the seven-day hold on the data is reasonable because the data held by WSDOT are anonymized, and therefore do not pose a risk to public privacy. However, SDOT's current operational policies do not reflect this practice.

Recommendation 3

Two Seattle Department of Transportation operational policies (License Plate Readers Surveillance Impact Report 12 and Condensed Surveillance Impact Report 4.0, 6) that address time frame regarding when the Washington State Department of Transportation deletes License Plate Readers data and for how long License Plate Readers data are stored should be updated to state that License Plate Readers data are anonymized by the Washington State Department of Transportation, which holds the data in temporary files for seven days.

Are the operational policies in the License Plate Readers SIR and CSIR documents in alignment concerning WSDOT's deletion of data?

No. CSIR 4.0, 6 is not an operational policy in the License Plate Readers (LPR) Surveillance Impact Report (SIR). The text is in LPR SIR 5.1 but is not expressly designated as an operational policy. As a result of these policy documents being out of alignment, there is an increased risk that policies missing from either document will not be enforced.

Recommendation 4

The Seattle Department of Transportation should resolve the discrepancy where the text for Condensed Surveillance Impact Report 4.0, 6 is not expressly designated as an operational policy in the License Plate Readers Surveillance Impact Report.

Is SDOT properly limiting access, storing, sharing, and using license plate data?

We were unable to determine whether SDOT is limiting access, storing, sharing, or using the license plate information it collects other than for use in traffic management purposes. **Operational Policy 8** states that only SDOT and WSDOT shall access LPR data. **Operational Policy 2** states that SDOT cannot store license plate numbers, **Operational Policy 13** states that license plate information collected by SDOT is not stored or shared other than for traffic management purposes, and **Operational Policy 11** states that no images of vehicles or occupants may be collected. Fully assessing the proper storage and sharing of the LPR data would require technical expertise that exceeded resources we had access to during this audit.

It is also possible that cybersecurity risks in SDOT's LPR system could result in LPR data being inadvertently or improperly shared with unauthorized parties and therefore could affect civil liberties.

Answering this question is important because of risks inherent in the current data sharing structure. We determined that the City has in-house resources that could do this type of assessment, and that this expertise is also provided by private contractors. The scope of this engagement should include follow-up on the implementation progress of recommendations from the 2015 SDOT Network Security Service Traffic Management Risk Report. We were not able to assess the implementation status of the recommendations from the 2015 report because it required technical expertise that exceeded resources we had access to during this audit.⁹

The Seattle Information Technology Department reported that they currently conduct enterprise security assessments and vulnerability scanning for the City as a whole.

Recommendation 5

The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.

⁹ We discuss the 2015 SDOT Network Security Service Traffic Management Risk Report in Section E: Complaints, Concerns, and Other Assessments

Compliance Summary: Technology and Data Sharing

Is SDOT in compliance with the relevant operational policies related to surveillance technology and data sharing?

Based on the evidence we reviewed, SDOT is not in compliance with three policies, is in compliance with two policies, and for three operational policies, we were unable to determine SDOT’s compliance because doing so was beyond the technical resources we had access to during this audit. The eight policies that are relevant in this context are show in Exhibit 2 below.

Exhibit 2: Operational Policies Compliance Matrix, Technology and Data Sharing

Operational Policy	Is SDOT in Compliance?	Recommendation(s)/ Comments
<p>Operational Policy 2: The SDOT LPR system is built strictly for traffic management and optimization. No raw data that includes license plate numbers is stored or used by SDOT or other departments or agencies for any other purposes. [Same as CSIR Operational Policy 2.0, 1]</p>	<p>NOT ASSESSED IN THIS AUDIT</p>	<p>Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle’s Information Technology Department or by an independent cybersecurity consultant.</p>
<p>Operational Policy 3: Each raw data record will be comprised of: time stamp, station identifier, camera channel, alphanumeric plate string, and confidence factor. [Same as CSIR Operational Policy 2.0, 2]</p>	<p>YES</p>	

Operational Policy	Is SDOT in Compliance?	Recommendation(s)/ Comments
<p>CSIR Operational Policy 4.0, 6: WSDOT immediately processes the travel time information, deletes the license plate numbers or source data, never storing any information about the license plates used to create them. [Not an Operational Policy in LPR SIR]</p>	<p>NO</p>	<p>Recommendation 3: Two Seattle Department of Transportation operational policies (License Plate Readers Surveillance Impact Report 12 and Condensed Surveillance Impact Report 4.0, 6) that address time frame regarding when the Washington State Department of Transportation deletes License Plate Readers data and for how long License Plate Readers data are stored should be updated to state that License Plate Readers data are anonymized by the Washington State Department of Transportation, which holds the data in temporary files for seven days.</p> <p>Recommendation 4: The Seattle Department of Transportation should resolve the discrepancy where the text for Condensed Surveillance Impact Report 4.0, 6 is not expressly designated as an operational policy in the License Plate Readers Surveillance Impact Report.</p>
<p>Operational Policy 8: Access to the data is only permitted to perform traffic analysis, conduct research, create reports, or connect to the API with software applications. No entity other than SDOT and WSDOT shall access or use the SDOT LPR data, other than processed data such as travel time data. [Same as CSIR 4.0, 2]</p>	<p>NOT ASSESSED IN THIS AUDIT</p>	<p>Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle’s Information Technology Department or by an independent cybersecurity consultant.</p>

Operational Policy	Is SDOT in Compliance?	Recommendation(s)/ Comments
<p>Operational Policy 12: License plate data is immediately deleted when the travel time is calculated by WSDOT and that calculated travel time is then sent back to SDOT. [Same as CSIR Operational Policy 3.0, 1]</p>	<p>NO</p>	<p>Recommendation 3: Two Seattle Department of Transportation operational policies (License Plate Readers Surveillance Impact Report 12 and Condensed Surveillance Impact Report 4.0, 6) that address time frame regarding when the Washington State Department of Transportation deletes License Plate Readers data and for how long License Plate Readers data are stored should be updated to state that License Plate Readers data are anonymized by the Washington State Department of Transportation, which holds the data in temporary files for seven days.</p>
<p>Operational Policy 13: No license plate information captured to create travel times is stored or used by SDOT, nor is it provided to other entities directly, or pooled into regional sharing systems and is only used for traffic management purposes. [Same as CSIR Operational Policy 3.0, 2]</p>	<p>NOT ASSESSED IN THIS AUDIT</p>	<p>Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle’s Information Technology Department or by an independent cybersecurity consultant.</p>
<p>Operational Policy 14: SDOT shares LPR data with the Washington State Department of Transportation (WSDOT) for the purpose of facilitating information processing and distribution of travel times between defined locations. SDOT and WSDOT must have a written agreement pertaining to sharing LPR data. [Same as CSIR Operational Policy 5.0, 1]</p>	<p>NO</p>	<p>Recommendation 2: The Seattle Department of Transportation should execute a written agreement with the Washington State Department of Transportation that, at a minimum, addresses data sharing, retention, and deletion of License Plate Readers data, including what the Washington State Department of Transportation can and cannot do with License Plate Readers data outside of its agreement with the Seattle Department of Transportation.</p>

Surveillance Usage Review: Seattle Department of Transportation License Plate Readers

Operational Policy	Is SDOT in Compliance?	Recommendation(s)/ Comments
Operational Policy 15: With respect to LPRs, with the exception of system set-up or troubleshooting, WSDOT shall share with SDOT only travel time information calculated as per the Surveillance Impact Report. [Same as CSIR Operational Policy 5.0, 2]	YES	

C. PROTOCOLS FOR DATA MANAGEMENT

Section Summary

To understand the extent to which data protocols for data management are safeguarding personal information, we interviewed knowledgeable SDOT Transportation Operations Center (TOC) officials. The SDOT TOC Manager and Senior Systems Engineer also demonstrated to us how an LPR camera is accessed and showed us the raw LPR data that is transmitted to WSDOT. We found that access to LPR cameras for the TOC technical team and Intelligent Transportation Systems (ITS) signal specialists is limited to device configuration and troubleshooting purposes. No images of vehicles and occupants are supposed to be collected by SDOT; however, we saw that in the process of capturing license plate images, the LPR cameras captured a sufficient amount of the body of the vehicles to be able to surmise the vehicle's color, make, and model. We also found that although the images are not transmitted to WSDOT, these images are held in the LPR cameras until they are automatically deleted.

Who installed the License Plate Readers cameras?

It is not clear who installed SDOT's LPR cameras. According to SDOT, the cameras were installed over ten years ago and SDOT does not know if the cameras were installed by SDOT contractors.

Were the cameras installed by qualified or authorized parties?

Not determined. Operational Policy 4 requires that LPR cameras be installed by qualified SDOT personnel or authorized electrical contractors. However, in the absence of records with details on who installed the cameras, we could not determine if the cameras were installed by qualified or authorized installers.

Will future cameras be installed in accordance with SDOT policy?

Not applicable. Because SDOT is no longer installing new LPR cameras, the policy is no longer applicable.

Who can access the License Plate Readers cameras?

LPR cameras are accessed by the SDOT TOC Technical Team and the SDOT ITS signal specialists. The SDOT TOC Technical Team can access the LPR cameras remotely for technical troubleshooting purposes, and the SDOT ITS signal specialists are deployed for in-person fixes to troubleshoot the cameras, such as moving a camera back into position if it has been unexpectedly moved out of position by wind.

Are access privileges in accordance with SDOT policy?

Access privileges are in accordance with one City policy, but not another. Based on the purpose of accessing the cameras, we determined that SDOT is in alignment with **Operational Policy 7**. This policy allows SDOT to access the LPR equipment for device configuration and troubleshooting. However, **Operational Policy 9A** limits access to the SDOT TOC Technical Team and does not explicitly allow SDOT ITS signal specialists to access the devices. Updating the policy to reflect the current operational practices will establish the LPR cameras privilege limits and ensure that the most appropriate practices are reflected in policy.

Recommendation 6

Operational Policy 9A (same as Condensed Surveillance Impact Report Operational Policy 4.0, 4) should be revised to reflect that License Plate Readers cameras are remotely accessible by the Seattle Department of Transportation’s Transportation Operations Center Technical Team and Intelligent Transportation System signal specialists for initial device configuration and issue troubleshooting purposes.

How is access to the License Plate Readers cameras protected?

Access to each LPR camera is protected by one username and password combination that is shared among the SDOT TOC Technical Team and ITS signal specialists. The system only supports one user account, so creating a separate user account for each person is not an option.

Is this control in compliance with SDOT policy?

The use of a username and password combination is in compliance with **Operational Policy 9B**. The policy requires that each device be protected by a username and password combination that is only known by SDOT staff.

Do the License Plate Readers cameras collect images of vehicles or the people in them?

SDOT told us that the LPR cameras are pre-set to capture only license plate images. However, when we met with the SDOT TOC Manager and Senior Systems Engineer who demonstrated to us how an LPR camera is accessed and the raw data that can be seen when it is accessed, we saw that the cameras captured portions of the body of cars as part of the license plates images. No images of vehicle occupants were visible, but the make and model of the vehicles could be surmised.

When a vehicle moves into view of an SDOT LPR camera, the camera captures an image of a portion of the vehicle. From this image, the camera applies an algorithm to locate the vehicle’s license plate and produces a smaller image of the license plate itself, which is read by the camera and processed into the raw data that is sent to WSDOT. The captured image shows enough of the body of the vehicle to

allow one to surmise the vehicle's color, make, and model. See Exhibit 3.

We asked SDOT if it is possible to direct the LPR camera to capture only the license plates and less of the vehicle body. SDOT told us that the camera needs to capture a field of view large enough to reliably locate and collect the license plate numbers to send to WSDOT. If the field of view is so small that the cameras cannot capture the license plates with their data to send to WSDOT, the result will be that the travel time information from WSDOT will be less reliable.

Exhibit 3: Sample Images from an SDOT LPR Camera



Source: Seattle Office of City Auditor
Note: license plates obscured by auditor.

Are the images kept in the License Plate Readers cameras or stored by SDOT?

Yes. We met with the SDOT TOC Senior Systems Engineer who told us that the images are retained in the LPR cameras in a buffer¹⁰ until they are automatically deleted. Because images are retained in the camera, security of these devices is important, potentially affecting civil liberties due to the images being inadvertently or improperly shared with unauthorized parties and should be included in the scope of **Recommendation 5**. Recommendation 5 states the Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.

Are the images transmitted to WSDOT?

No. SDOT told us that the LPR images do not leave the LPR camera. The images are processed into raw data (time stamp, station identifier, camera channel, alphanumeric plate string, and confidence factor) within the LPR camera itself and the raw data are what leaves the camera through SDOT's firewall to WSDOT.

¹⁰ A (data) buffer is a region of a physical memory storage used to temporarily store data. Source: [Wikipedia](https://en.wikipedia.org/wiki/Buffer_(computing)).

Is SDOT collecting images as set by policy?

Unclear. Operational Policy 11 states that the LPR cameras cannot collect images of vehicles or their occupants. We determined that the LPR cameras are capturing portions of vehicles surrounding the location of license plates and are not capturing images of vehicle occupants.

As stated earlier, the LPR cameras store the images for a period, but the policy is not clear as to what is meant by “images of vehicles.” For example, does this mean that other than capturing an image only of the license plate, that no other part of the vehicle can be captured in the image? Or is there a permissible amount of the vehicle that can be captured in the process of capturing its license plate image?

Furthermore, the policy is not included in the CSIR.

Recommendation 7

With respect to License Plate Readers Surveillance Impact Report Operational Policy 11, the Seattle Department of Transportation should clarify what is meant by “images of vehicles” and define the permissible extent of a vehicle’s image that can be captured in the process of capturing the license plate image.

Is the operational policy in the License Plate Readers SIR and CSIR documents in alignment concerning the collection of vehicle images or their occupants?

No. Operational Policy 11 in the LPR SIR prohibiting the collection of vehicle or occupant images is not included in the LPR CSIR. As a result of these policy documents being out of alignment, there is an increased risk that policies missing from either document will not be enforced.

Recommendation 8

The Seattle Department of Transportation should resolve the discrepancy where Operational Policy 11 in the License Plate Readers Surveillance Impact Report prohibiting the collection of vehicle or occupant images is not included in the License Plate Readers Condensed Surveillance Impact Report.

What is information collected by the License Plate Readers cameras used for?

As described earlier in this report, the information collected by LPR cameras is only used for system engineering, traffic planning, and public distribution purposes. The SDOT TOC Manager told us that public distribution of travel times comprises over 95 percent of LPR activities in the TOC, and the remaining five percent are for system engineering and traffic planning.

How are SDOT staff trained on proper handling of License Plate Readers data?

The TOC Technical Team and ITS signal specialists who have access to LPR cameras and the data in them are trained on-the-job.

The TOC Manager told us that some senior TOC Operators receive specialized training in addition to their normal training on using LPR and Acyclica technologies to add new travel routes to the DMS signs. The TOC Manager told us that the senior operators who receive the specialized training for adding new travel routes only access WSDOT-processed travel time information in their work; they do not access raw LPR data. **Operational Policy 16** refers to the additional training that TOC Operators receive to create new travel routes.

Is the training of SDOT staff in compliance with City policy?

Unclear. The TOC Manager told us that the training for the TOC Technical Team and ITS signal specialists is provided on-the-job. **Operational Policy 5** refers to “standard training” and **Operational Policy 6** refers only to training that should be provided to those who access or use LPR data. It appears that the training provided may be sufficient for operational purposes, but the operational policies are vague in terms of what the training needs to cover. Therefore, we could not determine whether the current training activities are sufficient for the purpose of protecting LPR data.

Is the training of WSDOT staff in compliance with SDOT policy?

No. WSDOT told us that there is no WSDOT training for handling SDOT LPR data as required by SDOT’s **Operational Policy 5** because there are no means for WSDOT personnel to access the LPR data, and the temporary files that hold anonymized data for seven days do not contain any humanly readable information.

Recommendation 9

The Seattle Department of Transportation should clearly define what is meant by “standard training” for those who access and use License Plate Readers data and develop criteria for determining who is required to take this training, including Washington State Department of Transportation employees.

Compliance Summary: Protocols for Data Management

Is SDOT in compliance with the relevant operational policies related to protocols for data management?

Based on the evidence we reviewed, SDOT is not compliance with four¹¹ operational policies, is in compliance with three¹² policies, and for one¹³ policy we were not able to determine compliance due to a lack of SDOT records. The eight policies are shown in Exhibit 4.

Exhibit 4: Operational Policies Compliance Matrix, Protocols for Data Management

Operational Policy	Is SDOT in compliance?	Recommendation(s)/ Comments
<p>Operational Policy 4: LPR cameras are installed by either qualified SDOT personnel, or authorized electrical contractors associated with a project. Except for third party vendors installing or maintaining a system, no entity other than SDOT and WSDOT shall access or use the SDOT LPR System. [Same as CSIR Operational Policy 4.0, 3]</p>	<p>NOT DETERMINED DUE TO LACK OF SDOT RECORDS</p>	<p>License Plate Readers cameras were installed about 10 years ago. The Seattle Department of Transportation (SDOT) does not have records as to whether the cameras were installed by SDOT or by SDOT contractors.</p>
<p>Operational Policy 5: SDOT shall develop standard training for operation of the LPR System in accordance with this Section and with any additional applicable SDOT policies, as should WSDOT, and only employees who have undergone such training may access or use the SDOT LPR System. [Same as CSIR Operational Policy 1.0, 2]</p>	<p>NO</p>	<p>Recommendation 9: The Seattle Department of Transportation should clearly define what is meant by “standard training” for those who access and use License Plate Readers data and develop criteria for determining who is required to take this training, including Washington State Department of Transportation employees.</p>

¹¹ OP 5, 6, 9A, 11

¹² OP 7, 9B, 16

¹³ OP 4

Surveillance Usage Review: Seattle Department of Transportation License Plate Readers

Operational Policy	Is SDOT in compliance?	Recommendation(s)/ Comments
<p>Operational Policy 6: Any City employee, whether an internal SDOT employee or other departmental user of the System, and those accessing data collected by the System, must complete training prior to using the System or accessing data collected by it. [Same as CSIR Operational Policy 1.0, 3]</p>	NO	<p>Recommendation 9: The Seattle Department of Transportation should clearly define what is meant by “standard training” for those who access and use License Plate Readers data and develop criteria for determining who is required to take this training, including Washington State Department of Transportation employees.</p>
<p>Operational Policy 7: Acceptable reasons for access to the equipment include initial device configuration and issue troubleshooting. [Same as CSIR Operational Policy 4.0, 1]</p>	YES	
<p>Operational Policy 9A: The LPR’s are remotely accessible only by members of the SDOT TOC Technical Team. [Same as CSIR Operational Policy 4.0, 4]</p>	NO	<p>Recommendation 6: Operational Policy 9A (same as Condensed Surveillance Impact Report Operational Policy 4.0, 4) should be revised to reflect that License Plate Readers cameras are remotely accessible by the Seattle Department of Transportation’s Transportation Operations Center Technical Team and Intelligent Transportation System signal specialists for initial device configuration and issue troubleshooting purposes.</p>
<p>Operational Policy 9B: Each device is protected by a username password combination that is only known by SDOT staff members. [Same as CSIR Operational Policy 4.0, 5]</p>	YES	

Operational Policy	Is SDOT in compliance?	Recommendation(s)/ Comments
<p>Operational Policy 11: No images of vehicles or occupants may be collected. [Not an Operational Policy in CSIR]</p>	<p>NO</p>	<p>We found that although images are not transmitted to WSDOT, vehicle images are held in the LPR cameras in a buffer until they are automatically deleted.</p> <p>Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle’s Information Technology Department or by an independent cybersecurity consultant.</p> <p>Recommendation 7: With respect to License Plate Readers Surveillance Impact Report Operational Policy 11, the Seattle Department of Transportation should clarify what is meant by “images of vehicles” and define the permissible extent of a vehicle’s image that can be captured in the process of capturing the license plate image.</p> <p>Recommendation 8: The Seattle Department of Transportation should resolve the discrepancy where Operational Policy 11 in the License Plate Readers Surveillance Impact Report prohibiting the collection of vehicle or occupant images is not included in the License Plate Readers Condensed Surveillance Impact Report.</p>
<p>Operational Policy 16: SDOT system users are trained on how to create new travel time routes. [Same as CSIR OP 5.0, 3]</p>	<p>YES</p>	

D. CIVIL LIBERTIES IMPACT

Section Summary

We could not conclude whether LPR technology had a negative effect on civil liberties or had disproportionate effects on disadvantaged populations because it required technical IT security expertise to which we did not have access during this audit, and because there was a lack of SDOT historical information about why LPR cameras were installed in a particular location. However, we mapped the locations of SDOT LPR cameras in Seattle, which indicated that SDOT placed LPR cameras in areas based on traffic volume, and that they are concentrated in two census tracts that have a high level of manufacturing and industrial activities with low population density. We note that the mapping did not include WSDOT cameras or SDOT's Acyclica technology, which could be used for surveillance purposes that affect civil liberties. We interviewed ACLU-Washington representatives about LPR technology civil liberties concerns, communicated with the SDOT Project Management Division about LPR deployment, and interviewed SDOT officials who manage and operate LPR technology.

Has the deployment of License Plate Readers cameras affected civil liberties?

Not known. LPR data being illegally, inadvertently or improperly accessed or shared with unauthorized parties, or used inappropriately, could impact civil liberties. As discussed in Section B, Data Sharing, we were unable to determine whether or not SDOT is limiting access, storing, sharing, or using LPR data securely because this would require technical expertise that was beyond the resources we had access to during this audit. When **Recommendation 5** is implemented, cybersecurity experts engaged by the Seattle Department of Transportation should conduct regular security assessments of License Plate Readers. These regular assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.

Has SDOT installed License Plate Readers cameras according to policy?

Not known. SDOT has installed LPR technology based on street transportation volumes and locations based on gaps in travel time coverage; however, records that document decisions for exactly where and why the cameras were installed in their locations are not available.

We communicated with an SDOT capital projects official in the Projects Development Division who explained how decisions are made to install new ITS elements, such as LPR cameras or Closed-Circuit Television (CCTV) cameras on key arterial streets. He explained that during SDOT's project development process, every

project has a "Complete Streets Checklist" that guides staff to review recommendations from its various strategic plans (e.g., Modal Master Plans such as the Bicycle Master Plan, safety plans, etc.), and to coordinate across SDOT divisions to implement the plans' recommendations as much as possible. The project development team also references the ITS Strategic Plan during project development and often incorporates ITS elements, such as LPR cameras or CCTV traffic cameras on key arterial streets if project funding allows.

The SDOT TOC Manager explained to us that because the goal of SDOT's LPR technology is to help as many people as possible get travel information for where they are going, LPR cameras were installed on key arterials with the highest volumes of traffic that would benefit from posted travel times. Although the LPR cameras were installed about 10 years ago, the TOC Manager told us that the key arterials in the ITS Strategic Plan have not changed.

However, detailed records for the decisions for exactly where and why the cameras were installed in their locations are no longer available. The TOC Manager also explained that there will not be any additional LPR cameras installed associated with travel time creation.

What are the civil liberties concerns about the License Plate Readers cameras?

License plate information identifies only a vehicle, but linked with other information about an individual, this knowledge is a perceived risk to privacy.¹⁴

Have there been any community concerns expressed regarding placement of License Plate Readers cameras?

We asked ACLU-Washington representatives if they were aware of any concerns expressed by any of ACLU's community partners regarding placement of LPR cameras in their communities, or if the ACLU had examined the LPR cameras' distribution in Seattle. They told us that they do not know all the locations where LPR cameras are deployed, but that a study of camera placements was worth considering. An ACLU-Washington representative commented that even if the technologies were placed relatively evenly across Seattle, a concern is that the data collected by the technologies might not be used in a proportionate manner.

The ACLU-Washington representative also commented that the general public might not know who to contact if they had concerns

¹⁴ License plate information is personally identifiable information. The National Institute of Standards and Technology (NIST) gives several definitions of "personally identifiable information." Included in all the NIST definitions is the characteristic that the information permits an individual to be identified by either direct or indirect means, or alone, or in combination with other linked information about the individual. Therefore, even if license plate information alone may not identify a specific person, according to the NIST definition, it is personally identifiable information.

about LPR cameras because they are not aware of the cameras' purpose and function. Furthermore, the cameras are not identified as belonging to the City (i.e., they are unmarked).

In their comments to the preliminary draft of this report section, the ACLU-Washington noted that there are many LPR operational policies that, if they are not complied with, could affect civil liberties. Examples are:

- The SDOT LPR System and the travel time information produced by it is used only for system engineering, traffic planning, and public distribution purpose. (Operational Policy 1)
- The SDOT LPR system is built strictly for traffic management and optimization. No raw data that includes license plate numbers is stored or used by SDOT or other departments or agencies for any other purposes. (Operational Policy 2)
- LPR cameras are installed by either qualified SDOT personnel, or authorized electrical contractors associated with a project. Except for third party vendors installing or maintaining a system, no entity other than SDOT or WSDOT shall access or use the SDOT LPR system. (Operational Policy 4)

Observations from Mapping

Mapping of LPR locations are shown on two census tract layers: 1) Population Density¹⁵ and 2) Race and Social Equity Composite Index.¹⁶ (See Appendices G and H)

We found that two census tracts, 93 and 109, have 42% of the LPRs in Seattle. These two census tracts are part of an industrial area that has a relatively low population density. SDOT told us that the LPRs in these census tracts are likely to capture trips coming from outlying residential neighborhoods to downtown Seattle. These LPRs help show commuters what other routes are less busy, which helps people coming to downtown from West Seattle and south of Seattle. Census tract 93 has a high population of disadvantaged residents. The remaining census tracts that contain LPRs have an average of three cameras.

SDOT told us that LPRs were placed in areas with the highest volumes of traffic with the intent that their placement would be useful to the largest number of commuters possible. LPRs offer alternative routes for travelers to consider, especially when drivers may need to shift their route off Interstate-5. SDOT told us they try to understand which corridors drivers are likely to be on so the drivers can make route decisions to continue to their destinations in the most efficient ways. In other words, LPRs were designed with a transportation focus to give commute information to the greatest possible number of travelers.

¹⁵ Population density was calculated at the census tract-level by the Seattle Office of Planning and Community Development using population estimates from the [American Community Survey 2013-2017](#) divided by gross land area.
¹⁶ The Racial and Social Equity Index is a census-tract based tool to assist with implementing the City's Race and Social Justice Initiative (RSJI) and to aid in the identification of neighborhoods of City planning, program and investment priorities. The index was compiled in 2018 by the City of Seattle Demographer in the Office of Planning and Community Development. The index combines the three equally weighted sub-indices described below, with census tracts categorized by five levels (quintiles) of priority/disadvantage.

- Race, English Language Learners, and Origins sub-index: ranks census tracts by an index of three measures weighted as follows: (shares of population who are)
 - Persons of color (weight: 1.0)
 - English language learners (weight: 0.5)
 - Foreign born (weight: 0.5)
- Socioeconomic Disadvantage sub-index: ranks census tracts by an index of two equally weighted measures: (shares of population with)
 - Income below 200 percent of poverty level
 - Educational attainment less than a bachelor's degree
- Health Disadvantage sub-index ranks census tracts by an index of seven equally weighted measures:
 - No leisure-time physical activity
 - Diagnosed diabetes
 - Obesity
 - Mental health not good
 - Asthma
 - Low life expectancy at birth
 - Disability

While the most disadvantaged (highest quintile and second highest quintile in the Race and Social Equity Index) census tracts do not have LPR cameras, many of the City’s LPR cameras are in areas with higher levels of disadvantage.

SDOT officials told us that the LPRs shown on these maps are not the only technology of this kind in the Seattle area. SDOT also uses a different technology, Acyclica, to capture commute times by reading license plates. For example, SDOT told us that they rely on Acyclica cameras in downtown, which is why there are fewer LPRs in this area. WSDOT has their own license plate reader cameras as well. Together, all these technologies help produce estimated commute times for people traveling in and out of the city. According to SDOT officials, the location of all these cameras needs to be considered to fully evaluate if license plate reader technologies are disproportionately impacting certain populations from a privacy and civil liberties perspective.

Compliance Summary: Civil Liberties Impact

Is SDOT in compliance with the relevant operational policy related to installation of License Plate Readers technology?

We were not able to determine compliance with the one operational policy concerning the technology’s civil liberties impact because SDOT could not provide documentation that describes how they chose where to locate the LPR cameras.

Exhibit 5: Operational Policies Compliance Matrix, Civil Liberties Impact

Operational Policy	Is SDOT in Compliance?	Recommendation(s)/ Comments
<p>Operational Policy 17: SDOT installs LPR based on street transportation volumes and locations based on gaps in travel time coverage along corridors identified in the SDOT ITS Strategic Plan. [Same as CSIR OP 6.0, 1]</p>	<p>NOT DETERMINED DUE TO LACK OF SDOT RECORDS</p>	<p>We were not able to determine compliance due to lack of Seattle Department of Transportation decision-making history regarding when and for what reasons each License Plate Readers camera was installed.</p>

E. COMPLAINTS, CONCERNS, AND OTHER ASSESSMENTS

Section Summary

We did not identify any privacy or civil liberties related complaints or concerns about the use of LPR technology received by the Seattle Department of Transportation or the City of Seattle’s Customer Service Bureau (CSB). We did not find any complaints related to LPRs in our review of complaints received by SDOT and the CSB between 2017-June 2020.

We found that one in-scope security assessment of the TOC system was conducted over the past five years. We were not able to assess the implementation status of the recommendations from this security assessment because it would require technical expertise that was beyond the resources we had access to during this audit.

Did SDOT receive complaints from the public about License Plate Readers technology privacy concerns?

No. We requested that SDOT provide us with copies of any complaints or concerns it had received from external parties (i.e., non-City of Seattle persons or entities) about the LPR technology. SDOT indicated they had not received any such complaints.

Did the City’s Customer Service Bureau receive complaints from the public about License Plate Readers technology privacy concerns?

No. We did not find any complaints or concerns related to privacy or civil liberties related to LPR cameras in the Customer Service Bureau (CSB) data. We examined complaints or concerns received by the City of Seattle through its Customer Service Bureau (CSB), which is part of the Department of Finance and Administrative Services. We obtained copies of the CSB’s General Inquiry Service Request data for January 2017 – June 2020. CSB uses a cloud-based hosted application to manage and track constituents’ service requests, suggestions, complaints and correspondence that are received in multiple ways, i.e., online, mobile app (“Find It, Fix It”), in person, phone, email, etc. Total CSB service requests for 2017 were 17,267, 27,239 for 2018, and 31,179 in 2019; and for January – June 2020 there were 11,234.¹⁷

¹⁷ 2020 Q1=5,472, 2020 Q2=5,762

Were there any internal audits or other assessments of code compliance concerning License Plate Readers technology?

Over the past five years there have been two security assessments of SDOT Transportation Operations Center (TOC) systems.

1. The more recent assessment examined major TOC systems and platforms, but not specific technologies used at the TOC, such as LPR cameras, and therefore was not in our scope.
2. The other assessment was a security assessment of SDOT's traffic management network comprised of the Transportation Operations Center and field networks of which the LPR system is a component. We were not able to assess the implementation status of the recommendations from this assessment because it would require information technology and cybersecurity technical expertise that was beyond the resources we had access to during this audit.

This follow-up work should be included as a part of **Recommendation 5** when cybersecurity experts are engaged to conduct regular security assessments.

F. COSTS

Section Summary

We estimated that SDOT’s LPR technology costs for 2020 will be about \$10,000. This includes fully loaded personnel and ongoing maintenance costs.

What are the costs for License Plate Readers technology?

SDOT estimated that the costs for the use of LPR technology in 2019 was \$2,377 and estimated that for January 2020 through June 2020 the total estimated cost was \$5,118.

	2019	Quarter 1- Quarter 2 2020
LPR Personnel Costs*	\$2,211	\$5,118
Maintenance & Replacement Costs	\$166	\$0
Total Costs	\$2,377	\$5,118

Source: Seattle Department of Transportation

*fully loaded labor costs

Based on the costs incurred in Quarter 1 (Q1) and Quarter 2 (Q2) of 2020, we estimated that the annual costs for 2020 will be about \$10,000 (i.e., \$5,118 X 2 for a full year). The bulk of the annual ongoing costs for LPR will be for personnel with minimal costs for equipment maintenance and replacement. As stated earlier, SDOT is no longer acquiring or installing new LPR cameras. When an LPR camera cannot be repaired, it will be replaced with an Acyclica sensor.

Personnel Costs

We asked SDOT why personnel costs projected for the full 2020 year are five times higher than for 2019. The SDOT TOC Manager explained to us that the TOC staff does not track personnel hours specifically to time spent working with the LPR system. To estimate personnel costs associated with the LPR system, the SDOT TOC Manager surveyed each TOC staff member to estimate the percentage of time spent working directly with the LPR system in 2019 through Q2 2020 and used the loaded labor costs for each position provided by SDOT Finance to calculate estimated personnel costs attributable to LPR technology. In 2019, the estimate totaled \$2,211 and for Q1-Q2 2020, the estimate totaled \$5,118.

Other Costs

Outside of the TOC personnel costs discussed above, costs for specific items, repair, and maintenance associated with the LPR system are tracked. For 2019, the cost for camera maintenance by the

SDOT traffic signal shop was \$166.¹⁸ In Q1 and Q2 of 2020, there were no costs outside of personnel costs associated with the LPR system.

¹⁸ Fully loaded labor costs.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

[Ordinance 125376](#) (the “Surveillance Ordinance”) requires the City Auditor to conduct an annual review of the City’s use of surveillance technologies by all City departments except the Seattle Police Department, and [Ordinance 125936](#) provided the City Council’s approval of the use of SDOT’s LPR technology.

Ordinance 125376 states that the review for non-Police surveillance technologies should include, but not be limited to the following:

- A. How surveillance technology has been used, how frequently, and whether usage patterns are changing over time;
- B. How often surveillance technology or its data are being shared with other entities, including other governments in particular;
- C. How well data management protocols are safeguarding individual information;
- D. How deployment of surveillance technologies impacted or could impact civil liberties or have disproportionate effects on disadvantaged populations, and how those impacts are being mitigated;
- E. A summary of any complaints or concerns received by or known by departments about their surveillance technology and results of any internal audits or other assessments of code compliance; and
- F. Total annual costs for use of surveillance technology, including personnel and other ongoing costs.

Scope

By ordinance,¹⁹ the scope of the usage review is to cover the data and activities of the previous year. Ordinance 125936 was signed by City Council in September 2019.

The scope of our audit was 2019 through June 2020. However, for Council question F, regarding complaints and concerns received by the department and others about LPR technology, we were able to examine data over the period of 2017 through June 2020.

¹⁹ Section 6 of Ordinance 125679 amended Section 5 of Ordinance 125376 (the Surveillance Ordinance) that requires that “surveillance usage reviews (in years subsequent to 2018) shall be filed in September (of the following year) and cover the data and activities of the previous year.” [Note: parens text added by auditor.]

Methodology

To accomplish the audit's objectives, we:

- Reviewed the 2018 LPR Surveillance Impact Report (SIR) and 2019 LPR Condensed Surveillance Impact Report (CSIR), amendments to Ordinance 125936;
- Attended two Surveillance Technology Public Comment meetings (October 25, 2018 and November 5, 2018) where SDOT LPR technology was discussed so that the public could learn about the technology and provide comments;
- Interviewed SDOT officials who manage and operate LPR technology;
- Communicated with WSDOT officials concerning the collection, processing, and deletion of LPR data;
- Interviewed ACLU-Washington representatives about civil liberties concerns about LPR technology;
- Interviewed Seattle Information Technology Department Cybersecurity/Risk Management officials about the work they have done or are doing to assess LPR technology security risks;
- Obtained data from the Department of Finance and Administrative Services Customer Service Division on constituent service requests, suggestions, complaints and correspondence received by the City of Seattle, and reviewed the data for complaints and concerns specific to LPR technology;
- Obtained location data for LPR cameras from the SDOT TOC and requested mapping and analysis of demographic information from Seattle Information Technology, GIS Products and Services; and
- Obtained cost data for the use of LPR technology.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX A

Department Response



Seattle
Department of
Transportation

December 11, 2020

David G. Jones, City Auditor
Seattle Office of City Auditor
700 5th Avenue, Suite 2410
Seattle, WA 98104

Re: License Plate Reader Surveillance Usage Review Departmental Response

Dear Mr. Jones,

Thank you for performing this thorough and collaborative audit of the Seattle Department of Transportation's (SDOT) use of License Plate Reader (LPR) cameras that empower everyday Seattleites to make informed decisions about their travel plans and our own experts to plan smarter on their behalf. While we are preparing to retire and upgrade this system by the end of 2021, we appreciate the time you and your staff took to examine and evaluate this complex information technology system and its use to notify travelers of real-time traffic conditions, so that its key finding can inform and shape our practices going forward.

We would like to highlight that the recommendations and items noted in the audit are primarily related to agreements and documentation, and not directly related to any risk to privacy data. With public safety as our number one priority, however, we can always stand to do better and promote practices that protect Seattleites in both the physical and digital domains.

SDOT's LPR technology is used for capturing license plate information to calculate the average travel time between two locations on Seattle's streets. Differing from other common LPR camera uses, the data from SDOT's LPR cameras is never shared with any law enforcement agency and they are never used for any law enforcement purpose. These LPR systems were initially acquired and installed in 2011. SDOT partners with the Washington State Department of Transportation (WSDOT) to process the data and produce travel time information. SDOT then shares the travel time information with the public on roadside electronic signs and through the [Travelers Information Map](#) so users can make more informed trip decisions. SDOT also uses travel times for its own system engineering and traffic planning purposes. While the LPR system has been an important tool for providing real-time information, the equipment is becoming obsolete and we intend to replace all of the LPR equipment with a different type of sensor by the end of 2021. These Acyclica sensors are undergoing the surveillance evaluation process, and WSDOT will not have any involvement with the data from those sensors.

They Acyclica system differs from the existing LPR system because they are small sensors installed in traffic signal control boxes. They identify when Wi-Fi-enabled devices in vehicles, like phones, move past different locations. And by measuring the time it took they can provide SDOT back a travel time. Compared to LPR cameras, Acyclica sensors are also considerably less expensive and they can be deployed and maintained using fewer labor resources.

We concur with all 9 of the recommendations described in Appendix B and plan to take specific actions, to address each of them in the ways briefly outlined as follows.

Of the recommendations in which we are in concurrence, six of them (recommendations 1,3,4,6,7 and 8) are all related to SDOT resolving text discrepancies within the Condensed Surveillance Impact Report (CSIR) and the License Plate Readers Surveillance Impact Report (SIR). In response to all six, SDOT will coordinate with the Seattle Information Technology Department (ITD) Privacy Team, which managed the production of the LPR SIR and CSIR, to revise these reports as recommended. This demonstrates that SDOT is taking necessary steps to ensure that there are no discrepancies between documents which dictate our use of LPR cameras.

Recommendation 5 states that SDOT should engage cybersecurity experts to conduct regular security assessments that specifically address data security and the risk of LPR data being inadvertently or improperly shared. We concur and already have an active engagement with assigned ITD cybersecurity experts. This includes recurring meetings to review practices and technologies while providing guidance for improving SDOT's overall security posture.

The two remaining recommendations (2 and 9) primarily relate to the existing methods and procedures SDOT and WSDOT use to produce travel times using LPR technology. Recommendation 2 states that SDOT should execute a written agreement with WSDOT that, at a minimum, addresses data sharing, retention, and deletion of LPR data, including what the WSDOT can and cannot do with LPR data outside of its agreement with the SDOT. Recommendation 9 states that SDOT should clearly define what is meant by "standard training" for those who access and use LPR data and develop criteria for determining who is required to take this training, including WSDOT employees.

SDOT has had numerous conversations with WSDOT over the past year about how to proceed with the LPR program. Options discussed included migrating the travel time processing software from WSDOT to SDOT and/or creating a data sharing agreement and training program. It became clear, however, that creating a data sharing agreement and other necessary alignments would require a sizeable, SDOT-funded investment to support these efforts. With the size and the complexity of the investment bumping up against SDOT's LPR camera systems nearing "end-of-life" status and are no longer supported by the manufacturer (PIPS), SDOT made the fiscally prudent and strategic decision to instead expedite efforts already underway to our current LPR cameras with Acyclica sensors that provide the same travel time information without the need for additional SDOT investments in WSDOT systems. SDOT will complete the replacement of every LPR system by the end of 2021 with an Acyclica sensor.

We look forward to working with you to review our use of technologies defined by the Surveillance Ordinance, while continuing to develop, maintain, and operate a transportation system that promotes the mobility of people and goods, and enhances the quality of life, environment, and economy of Seattle.

Sincerely,



Sam Zimbabwe (Dec 11, 2020 16:21 PST)

Sam Zimbabwe
Director

APPENDIX B

List of Recommendations

<p>Recommendation 1: The Seattle Department of Transportation should remove the word “enforcement,” from Surveillance Impact Report Operational Policy 10 and Condensed Surveillance Impact Report Operational Policy 5.0, 4, and revise the references to this work to clarify that it refers to work zone congestion analysis and not enforcement.</p>
<p>SDOT Concurrence: Concur</p>
<p>SDOT will coordinate with the ITD Privacy Team which managed the production of the LPR SIR and CSIR to revise these documents as recommended.</p>
<p>Recommendation 2: The Seattle Department of Transportation should execute a written agreement with the Washington State Department of Transportation that, at a minimum, addresses data sharing, retention, and deletion of License Plate Readers data, including what the Washington State Department of Transportation can and cannot do with License Plate Readers data outside of its agreement with the Seattle Department of Transportation.</p>
<p>SDOT Concurrence: Concur</p>
<p>SDOT has had numerous conversations with WSDOT about how to proceed with this program. Options discussed included migrating the travel time processing software from WSDOT to SDOT and/or creating a data sharing agreement. Based on those conversations, it was determined that creating an agreement would require an SDOT funded investment to support WSDOT’s multi-departmental review team (IT, Law, Transportation). Additionally, the report suggests that SDOT and WSDOT should create standard LPR training programs which would require investments from both departments. Recognizing these critical factors, SDOT decided to not prolong the replacement work and avoid allocating scarce resources to support an unsustainable program. In response, SDOT will complete the replacement of every LPR system by the end of 2021.</p>
<p>Recommendation 3: Two Seattle Department of Transportation operational policies (License Plate Readers Surveillance Impact Report 12 and Condensed Surveillance Impact Report 4.0, 6), that address time frame regarding when the Washington State Department of Transportation deletes License Plate Readers data and for how long License Plate Readers data are stored, should be updated to state that License Plate Readers data are anonymized by the Washington State Department of Transportation, which holds the data in temporary files for seven days.</p>
<p>SDOT Concurrence: Concur</p>
<p>SDOT will coordinate with the ITD Privacy Team which managed the production of the LPR SIR and CSIR to revise these documents as recommended.</p>

<p>Recommendation 4: The Seattle Department of Transportation should resolve the discrepancy where the text for Condensed Surveillance Impact Report 4.0, 6 is not expressly designated as an operational policy in the License Plate Readers Surveillance Impact Report.</p>
<p>SDOT Concurrence: Concur</p>
<p>SDOT will coordinate with the ITD Privacy Team which managed the production of the LPR SIR and CSIR to revise these documents as recommended.</p>
<p>Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security risk report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle’s Information Technology Department or by an independent cybersecurity consultant.</p>
<p>SDOT Concurrence: Concur</p>
<p>SDOT already has an active engagement with assigned ITD cybersecurity experts. This includes recurring meetings to review practices and technologies while providing guidance for improving SDOT’s overall security posture.</p>
<p>Recommendation 6: Operational Policy 9A (same as Condensed Surveillance Impact Report Operational Policy 4.0, 4) should be revised to reflect that License Plate Readers cameras are remotely accessible by the Seattle Department of Transportation’s Transportation Operations Center Technical Team and Intelligent Transportation System signal specialists for initial device configuration and issue troubleshooting purposes.</p>
<p>SDOT Concurrence: Concur</p>
<p>SDOT will coordinate with the ITD Privacy Team which managed the production of the LPR SIR and CSIR to revise these documents as recommended.</p>
<p>Recommendation 7: With respect to License Plate Readers Surveillance Impact Report Operational Policy 11, the Seattle Department of Transportation should clarify what is meant by “images of vehicles” and define the permissible extent of a vehicle’s image that can be captured in the process of capturing the license plate image.</p>
<p>SDOT Concurrence: Concur</p>
<p>SDOT will coordinate with the ITD Privacy Team which managed the production of the LPR SIR and CSIR to revise these documents as recommended.</p>

Recommendation 8: The Seattle Department of Transportation should resolve the discrepancy where Operational Policy 11 in the License Plate Readers Surveillance Impact Report prohibiting the collection of vehicle or occupant images is not included in the License Plate Readers Condensed Surveillance Impact Report.

SDOT Concurrence: Concur

SDOT will coordinate with the ITD Privacy Team which managed the production of the LPR SIR and CSIR to revise these documents as recommended.

Recommendation 9: The Seattle Department of Transportation should clearly define what is meant by “standard training” for those who access and use License Plate Readers data and develop criteria for determining who is required to take this training, including Washington State Department of Transportation employees.

SDOT Concurrence: Concur

SDOT will clearly define what is meant by “standard training” for those who access and use LPR data and determine who is required to take this training.

APPENDIX C

Operational Policies Cross-Referencing Matrix

We used the operational policy statements in the LPR Surveillance Impact Report (SIR) and LPR Condensed Surveillance Impact Report (CSIR) as the criteria to assess the evidence we gathered (e.g., from interviews) about whether the technology was being used in accordance with legislative requirements.

The LPR Surveillance Impact Report²⁰ accepted by Ordinance 125936 (9/23/2019) does not define “operational policy,” although there are numerous operational policy statements in it. The LPR²¹ CSIR states that “the boldface Operational Policies contained (in the CSIR) constitute the enforceable policies and procedures applicable to SDOT License Plate Readers, as set forth in SMC 14.18 and are enforceable via SMC 14.18.070.”

The LPR SIR’s operational policies are not numbered whereas the ones listed in the LPR CSIR are numbered. The following table shows the numbers we assigned for the operational policies in the LPR SIR in the sequence as they appeared in the document. And for each operational policy in the LPR SIR, we also noted the associated operational policy in the LPR CSIR.

Please refer to the chart below for how we numbered the operational policies in the LPR SIR and the corresponding operational policy number in the LPR CSIR.

LPR Surveillance Impact Report	LPR Condensed Surveillance Impact Report
Text is in SIR 5.1 but is not an Operational Policy.	OP 4.0, 6: WSDOT immediately processes the travel time information, deletes the license plate numbers or source data, never storing any information about the license plates used to create them.
Operational Policy 1 The SDOT LPR System and the travel time information produced by it is used only for system engineering, traffic planning, and public distribution purposes. [1.0]	OP 1.0, 1
Operational Policy 2 The SDOT LPR system is built strictly for traffic management and optimization. No raw data that includes license plate numbers is stored or used by SDOT or other departments or agencies for any other purposes. [2.0]	OP 2.0, 1

²⁰ [Att 1 – Surveillance Impact Report: License Plate Readers v2](#), 2018 Surveillance Impact Report SDOT License Plate Readers (September 23, 2019 Attachment 1 to Ordinance 125936)

²¹ [Att 3 - 2019 Condensed Surveillance Impact Report: License Plate Readers](#), 2019 Condensed Surveillance Impact Report (CSIR) SDOT License Plate Readers (September 23, 2019 Attachment 3 to Ordinance 125936)

LPR Surveillance Impact Report	LPR Condensed Surveillance Impact Report
<p>Operational Policy 3 Each raw data record will be comprised of: time stamp, station identifier, cameral channel, alphanumeric plate string, and confidence factor. [2.0]</p>	<p>OP 2.0, 2</p>
<p>Operational Policy 4 LPR cameras are installed by either qualified SDOT personnel, or authorized electrical contractors associated with a project. Except for third party vendors installing or maintaining a system, no entity other than SDOT or WSDOT shall access or use the SDOT LPR System. [2.0]</p>	<p>OP 4.0, 3</p>
<p>Operational Policy 5 SDOT shall develop standard training for operation of the LPR System in accordance with this Section and with any additional applicable SDOT policies, as should WSDOT, and only employees who have undergone such training may access or use the SDOT LPR System. [3.0]</p>	<p>OP 1.0, 2</p>
<p>Operational Policy 6 Any City employee, whether an internal SDOT employee or other departmental user of the System, and those accessing data collected by the System, must complete training prior to using the System or accessing data collected by it. [3.0]</p>	<p>OP 1.0, 3</p>
<p>Operational Policy 7 Acceptable reasons for access to the equipment include initial device configuration and issue troubleshooting. [3.0]</p>	<p>OP 4.0, 1</p>
<p>Operational Policy 8 Access to the data is only permitted to perform traffic analysis, conduct research, create reports, or connect to the Application Programming Interface (API) with software applications. No entity other than SDOT and WSDOT shall access to use the SDOT LPR data, other than processed data such as travel time data. [3.0]</p>	<p>OP 4.0, 2</p>

LPR Surveillance Impact Report	LPR Condensed Surveillance Impact Report
<p>[Note: We divided the Operational Policy as 9A and 9B; the SIR shows this as one operational policy.]</p> <p>Operational Policy 9A The LPR's are remotely accessible only by members of the SDOT TOC Technical Team.</p> <p>Operational Policy 9B Each device is protected by a username password combination that is only known by SDOT staff members. [3.0]</p>	<p>These are separate CSIR operational policies; in the LPR SIR, the two CSIR operational policies are combined into one operational policy (Operational Policy 9).</p> <p>OP 4.0, 4: The LPRs are remotely accessible only by members of the SDOT TOC Technical Team.</p> <p>OP 4.0, 5: Each device is protected by a username password combination that is only known by SDOT staff members.</p>
<p>Operational Policy 10 Applications of travel time information in the Department include: signal timing and coordination, traffic network optimization, street parking congestion analysis, congestion mapping, route planning, work zone congestion enforcement, variable message signs, incident detection, emergency responder routing and route utilization. [3.0]</p>	<p>OP 5.0, 4</p>
<p>Operational Policy 11 No images of vehicles or occupants may be collected. [4.0]</p>	<p>No CSIR OP for this SIR OP</p>
<p>Operational Policy 12 License plate data is immediately deleted when the travel time is calculated by WSDOT and that calculated travel time is then sent back to SDOT. [5.0]</p>	<p>OP 3.0, 1</p>
<p>Operational Policy 13 No license plate information captured to create travel times is stored or used by SDOT, nor is it provided to other entities directly, or pooled into regional sharing systems and is only used for traffic management purposes. [5.0]</p>	<p>OP 3.0, 2</p>

LPR Surveillance Impact Report	LPR Condensed Surveillance Impact Report
<p>Operational Policy 14 SDOT shares LPR data with the Washington State Department of Transportation (WSDOT) for the purpose of facilitating information processing and distribution of travel times between defined locations. SDOT and WSDOT must have a written agreement pertaining to sharing LPR data. [6.0]</p>	<p>OP 5.0, 1</p>
<p>Operational Policy 15 With respect to LPRs, with the exception of system set-up or troubleshooting, WSDOT shall share with SDOT only travel time information calculated as per the Surveillance Impact Report. [6.0]</p>	<p>OP 5.0, 2</p>
<p>Operational Policy 16 SDOT system users are trained on how to create new travel time routes. [7.0]</p>	<p>OP 5.0, 3</p>
<p>Operational Policy 17 SDOT installs LPR based on street transportation volumes and locations based on gaps in travel time coverage along corridors identified in the SDOT ITS Strategic Plan. [RACIAL EQUITY TOOLKIT 2.0]</p>	<p>OP 6.0, 1</p>

APPENDIX D

Operational Policies Compliance Matrix (consolidated for all report sections)

Report Section	Operational Policy	Is SDOT in compliance?	Recommendation(s)/ Comments
LPR Use	Operational Policy 1: The SDOT LPR System and the travel time information produced by it is used only for system engineering, traffic planning, and public distribution purposes. [Same as CSIR Operational Policy 1.0, 1]	YES	
	Operational Policy 10: Applications of travel time information in the Department include: signal timing and coordination, traffic network optimization, street parking, congestion analysis, congestion mapping, route planning, work zone congestion enforcement, variable message signs, incident detection, emergency responder routing and route utilization. [Same as CSIR Operational Policy 5.0, 4]	YES	We assessed that SDOT is not out of compliance with the Operational Policy but that the wording of the policy needs to be corrected to be consistent with SDOT's practice. Recommendation 1: The Seattle Department of Transportation should remove the word "enforcement," from Surveillance Impact Report Operational Policy 10 and Condensed Surveillance Impact Report Operational Policy 5.0, 4, and revise the references to this work to clarify that it refers to work zone congestion analysis and not enforcement.
Data Sharing	Operational Policy 2: The SDOT LPR system is built strictly for traffic management and optimization. No raw data that includes license plate numbers is stored or used by SDOT or other departments or agencies for any other purposes. [Same as CSIR Operational Policy 2.0, 1]	NOT ASSESSED IN THIS AUDIT	Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.
	Operational Policy 3: Each raw data record will be comprised of: Time stamp, station identifier, camera channel, alphanumeric plate string, and confidence factor. [Same as CSIR Operational Policy 2.0, 2]	YES	
	CSIR Operational Policy 4.0, 6: WSDOT immediately processes the travel time information, deletes the license plate numbers or source data, never storing any information about the license plates used to create them. [Not an Operational Policy in LPR SIR]	NO	Recommendation 3: Two Seattle Department of Transportation operational policies (License Plate Readers Surveillance Impact Report 12 and Condensed Surveillance Impact Report 4.0, 6) that address time frame regarding when the Washington State Department of Transportation deletes License Plate Readers data and for how long License Plate Readers data are stored should be updated to state that License Plate Readers data are anonymized by the Washington State Department of Transportation, which holds the data in temporary files for seven days. Recommendation 4: The Seattle Department of Transportation should resolve the discrepancy where the text for Condensed Surveillance Impact Report 4.0, 6 is not expressly designated as an operational policy in the License Plate Readers Surveillance Impact Report.
	Operational Policy 8: Access to the data is only permitted to perform traffic analysis, conduct research, create reports, or connect to the API with software applications. No entity other than SDOT and WSDOT shall access or use the SDOT LPR data, other than processed data such as travel time data. [Same as CSIR 4.0, 2]	NOT ASSESSED IN THIS AUDIT	Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.
	Operational Policy 12: License plate data is immediately deleted when the travel time is calculated by WSDOT and that calculated travel time is then sent back to SDOT. [Same as CSIR Operational Policy 3.0, 1]	NO	Recommendation 3: Two Seattle Department of Transportation operational policies (License Plate Readers Surveillance Impact Report 12 and Condensed Surveillance Impact Report 4.0, 6) that address time frame regarding when the Washington State Department of Transportation deletes License Plate Readers data and for how long License Plate Readers data are stored should be updated to state that License Plate Readers data are anonymized by the Washington State Department of Transportation, which holds the data in temporary files for seven days.
	Operational Policy 13: No license plate information captured to create travel times is stored or used by SDOT, nor is it provided to other entities directly, or pooled into regional sharing systems and is only used for traffic management purposes. [Same as CSIR Operational Policy 3.0, 2]	NOT ASSESSED IN THIS AUDIT	Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.
	Operational Policy 14: SDOT shares LPR data with the Washington State Department of Transportation (WSDOT) for the purpose of facilitating information processing and distribution of travel times between defined locations. SDOT and WSDOT must have a written agreement pertaining to sharing LPR data. [Same as CSIR Operational Policy 5.0, 1]	NO	Recommendation 2: The Seattle Department of Transportation should execute a written agreement with the Washington State Department of Transportation that, at a minimum, addresses data sharing, retention, and deletion of License Plate Readers data, including what the Washington State Department of Transportation can and cannot do with License Plate Readers data outside of its agreement with the Seattle Department of Transportation.

Surveillance Usage Review: Seattle Department of Transportation License Plate Readers

Report Section	Operational Policy	Is SDOT in compliance?	Recommendation(s)/ Comments
	Operational Policy 15: With respect to LPRs, with the exception of system set-up or troubleshooting, WSDOT shall share with SDOT only travel time information calculated as per the Surveillance Impact Report. [Same as CSIR Operational Policy 5.0, 2]	YES	
Data Management	Operational Policy 4: LPR cameras are installed by either qualified SDOT personnel, or authorized electrical contractors associated with a project. Except for third party vendors installing or maintaining a system, no entity other than SDOT and WSDOT shall access or use the SDOT LPR System. [Same as CSIR Operational Policy 4.0, 3]	NOT DETERMINED DUE TO LACK OF SDOT RECORDS	License Plate Readers cameras were installed about 10 years ago. The Seattle Department of Transportation (SDOT) does not have records as to whether the cameras were installed by SDOT or by SDOT contractors.
	Operational Policy 5: SDOT shall develop standard training for operation of the LPR System in accordance with this Section and with any additional applicable SDOT policies, as should WSDOT, and only employees who have undergone such training may access or use the SDOT LPR System. [Same as CSIR Operational Policy 1.0, 2]	NO	Recommendation 9: The Seattle Department of Transportation should clearly define what is meant by "standard training" for those who access and use License Plate Readers data and develop criteria for determining who is required to take this training, including the Washington State Department of Transportation employees.
	Operational Policy 6: Any City employee, whether an internal SDOT employee or other departmental user of the System, and those accessing data collected by the System, must complete training prior to using the System or accessing data collected by it. [Same as CSIR Operational Policy 1.0, 3]	NO	Recommendation 9: The Seattle Department of Transportation should clearly define what is meant by "standard training" for those who access and use License Plate Readers data and develop criteria for determining who is required to take this training, including Washington State Department of Transportation employees.
	Operational Policy 7: Acceptable reasons for access to the equipment include initial device configuration and issue troubleshooting. [Same as CSIR Operational Policy 4.0, 1]	YES	
	Operational Policy 9A: The LPR's are remotely accessible only by members of the SDOT TOC Technical Team. [Same as CSIR Operational Policy 4.0, 4]	NO	Recommendation 6: Operational Policy 9A (same as Condensed Surveillance Impact Report Operational Policy 4.0, 4) should be revised to reflect that License Plate Readers cameras are remotely accessible by the Seattle Department of Transportation's Transportation Operations Center Technical Team and Intelligent Transportation System signal specialists for initial device configuration and issue troubleshooting purposes.
	Operational Policy 9B: Each device is protected by a username password combination that is only known by SDOT staff members. [Same as CSIR Operational Policy 4.0, 5]	YES	
	Operational Policy 11: No images of vehicles or occupants may be collected. [Not an Operational Policy in CSIR]	NO	<p>We found that although images are not transmitted to WSDOT, vehicle images are held in the LPR cameras in a buffer until they are automatically deleted.</p> <p>Recommendation 5: The Seattle Department of Transportation should engage cybersecurity experts to conduct regular security assessments of License Plate Readers and to follow-up on the implementation progress of a 2015 network security report. The regular security assessments should specifically address data security and the risk of LPR data being inadvertently or improperly shared. This work could be done by the City of Seattle's Information Technology Department or by an independent cybersecurity consultant.</p> <p>Recommendation 7: With respect to License Plate Readers Surveillance Impact Report Operational Policy 11, the Seattle Department of Transportation should clarify what is meant by "images of vehicles" and define the permissible extent of a vehicle's image that can be captured in the process of capturing the license plate image.</p> <p>Recommendation 8: The Seattle Department of Transportation should resolve the discrepancy where Operational Policy 11 in the License Plate Readers Surveillance Impact Report prohibiting the collection of vehicle or occupant images is not included in the License Plate Readers Condensed Surveillance Impact Report.</p>
	Operational Policy 16: SDOT system users are trained on how to create new travel time routes. [Same as CSIR OP 5.0, 3]	YES	
Civil Liberties Impact	Operational Policy 17: SDOT installs LPR based on street transportation volumes and locations based on gaps in travel time coverage along corridors identified in the SDOT ITS Strategic Plan. [Same as CSIR OP 6.0, 1]	NOT DETERMINED DUE TO LACK OF SDOT RECORDS	We were not able to determine compliance due to lack of Seattle Department of Transportation decision-making history regarding when and for what reasons each License Plate Readers camera was installed.

APPENDIX E

License Plate Readers (LPR) Technology

SDOT's LPR Technology

SDOT's LPR technology is primarily used for determining travel times by automobiles between certain points on Seattle's streets. SDOT shares this information with the public by roadside electronic signs and through the [Traveler Information Web Map](#) so that individuals can make informed trip decisions. SDOT also uses the travel times for its own system engineering²² and traffic planning²³ purposes.

The LPR Surveillance Impact Report (SIR) states that SDOT initially acquired the technology in 2011 through a federal grant and deployed it in 2012.²⁴ SDOT's LPR technology is part of the City of Seattle's Intelligent Transportation System (ITS),²⁵ which uses electronics and communications technologies to enhance mobility for all transportation modes by increasing the efficiency and safety of the transportation infrastructure.²⁶

According to the LPR SIR, LPR technology is a combination of hardware and software used for capturing and monitoring images of license plates. LPR cameras are installed on dedicated mast arms that are connected to signal poles and positioned over travel lanes at various intersections throughout Seattle. Electrical power is provided from the nearest traffic signal cabinet.

The cameras are high definition cameras specifically designed to capture images of license plates as they move into view. Images of the license plates are processed by software that reports the license plate number to the Washington State Department of Transportation (WSDOT) with a time stamp, plate number, LPR camera channel, and station (intersection) identifier. WSDOT processes the travel time between intersections and sends the information back to SDOT.²⁷

Exhibit 6 shows at a high level how SDOT provides LPR data to WSDOT for processing so that WSDOT can provide SDOT with travel time information.

²² System engineering in this context is evaluating and applying travel time data to determine solutions to make the streets work better, e.g., improving traffic flow for particular transportation modes such as busses and bicycles.

²³ An example of traffic planning would be verifying the effectiveness of an operational change such as signal timing adjustments.

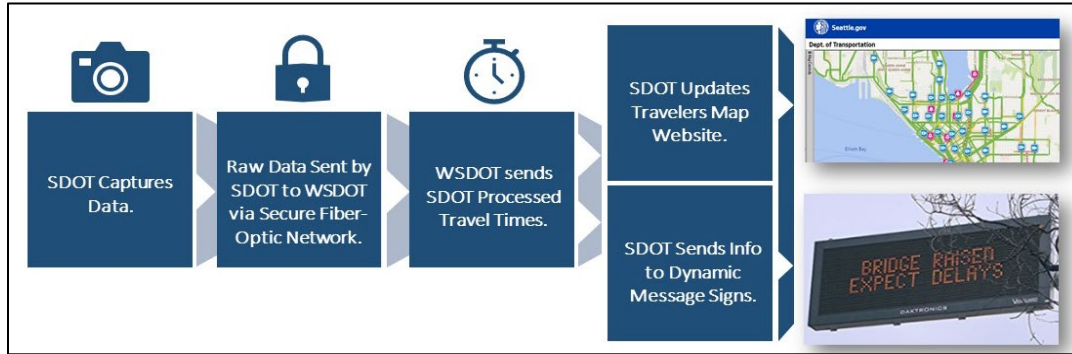
²⁴ LPR SIR Financial Information 1.0

²⁵ ITS core investments and infrastructure include: traffic signal controllers, cabinets, detection and displays; the citywide ITS communications network; traffic cameras that enable staff to view operations and dynamically adjust traffic signal timing if needed; DMS that provide on-street traveler information; the traveler's website (www.seattle.gov/travelers) that includes congestion information, traffic advisories and traffic camera images; the Traffic Operations Center (TOC) that includes processing, monitoring, and communications equipment allowing staff to interact with the systems; and the staff that operate and maintain these assets. Source: [ITS Strategic Plan](#), p. 1)

²⁶ [ITS Strategic Plan](#), Overview, p. 1

²⁷ SDOT LPR Fact Sheet

Exhibit 6: How SDOT provides LPR data to WSDOT



Source: Seattle Office of City Auditor

LPR cameras are owned and operated by SDOT²⁸ and have no markings that indicate that they are in use, and there is no signage that indicates ownership or contact information.²⁹

SDOT uses PIPS P372 LPR cameras. According to the SIR:³⁰

- “the P372 is a single or dual camera complete with video processing/ control/Automatic License Plate Readers (ALPR). The P372 is enclosed in a rugged extruded aluminum housing sealed to IP67. The P372 detects the retro reflective return from a license plate in hardware using digital signal processing algorithms and captures the field containing the best image of the license plate. The P372 stream the captured image to the software ALPR engine that performs optical character recognition on the image and reports the license plate number with an associated confidence of the result.”
- “the LPRs are programmed with an IP address, and they communicate by being physically connected to the SDOT ITS Network switch located in (the nearest traffic) cabinet.”
- “On detection of a vehicle, the P372 will send a message to the Washington State Department of Transportation (WSDOT) host comprising time stamp and tag details. The connection to the host is opened on the first plate and thereafter maintained open until no vehicles have been detected for a period, at which time the connection will be closed.”
- “SDOT and WSDOT have established an intergovernmental data network to facilitate the sharing of information. This occurs by a WSDOT network router being installed near an SDOT network router in the Seattle Municipal Tower. These two networks are separated by an SDOT managed firewall that is responsible for filtering the data traffic. This firewall translates each LPR’s IP address so it can be sent to the WSDOT host computer for processing. WSDOT computer systems match the number plates and return the average travel time difference between plate readings. WSDOT does not archive the plate data. After the matching process, the plate information is deleted automatically from WSDOT’s traffic system.”

²⁸ LPR SIR 4.8

²⁹ LPR SIR 4.6

³⁰ LPR SIR 2.3

- “SDOT then receives the travel times back from WSDOT from the publicly available Application Programming Interface (API). That API is consumed by a custom built SDOT software which then feeds the relevant data into our Cameleon ITS sign control software. Cameleon ITS then sends travel time information to SDOT Dynamic Message Signs (DMS³¹).”

Commercial and Open Source LPRs

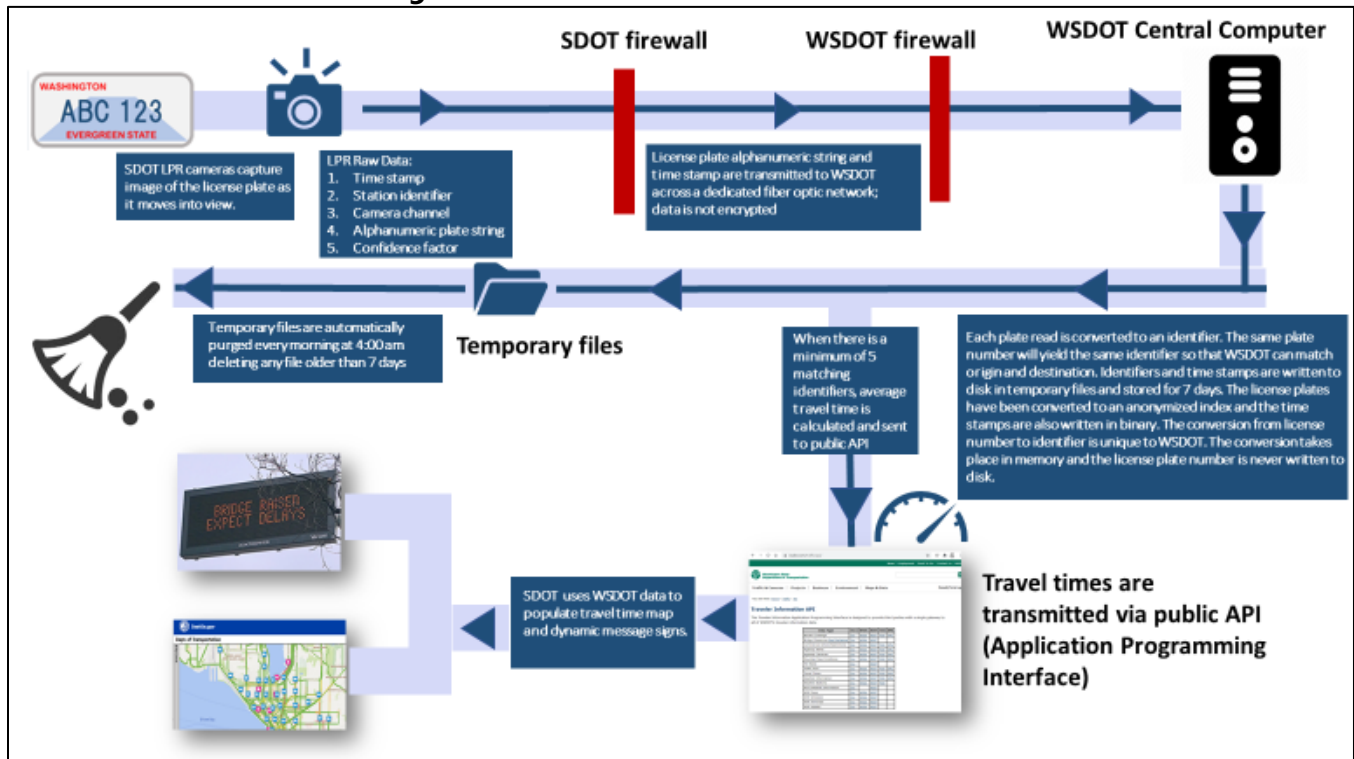
If someone wanted to obtain license plate and location data for their own surveillance purposes, license plate information is readily available for purchase commercially. For example, [Digital Recognition Network](#) (DRN) is a Fort Worth, Texas company that is a provider of license plate recognition systems, and according to its website, it sells license plate information to insurance companies, private investigators, and auto repossession agents. Its website also says that DRN is a partner company to [Vigilant Solutions](#), which provides license plate scans to law enforcement, including police and U.S. Immigration and Customs Enforcement. There are also open source solutions where, with access to recorded images, one could set up one’s own LPR system. Examples are: [OpenALPR](#), [Watchman](#), and [ispyconnect](#).

³¹ “DMS are the large, electronic signs which overhang or appear along major streets throughout Seattle. The signs are typically used to display information about traffic conditions travel times, construction, and road incidents. Travel time information is the default message that appears on a DMS daily from 5AM-9AM, and 4PM-7PM along 12 corridors. With this type of information displayed, drivers can make real time route choices given the traffic conditions ahead. Recently, SDOT has begun to combine the LPR travel time data with SDOT’s other travel time technology (Acyclica) to provide information to even more destinations. SDOT also provides travel time information on the [Traveler Information Map](#) web application.” (Traffic Cameras SIR 2.3)

APPENDIX F

SDOT-WSDOT Data Sharing (How SDOT Shares LPR Data with WSDOT)

Exhibit 7: LPR Data Flow Diagram



Source: Seattle Office of City Auditor

SDOT’s LPR cameras capture images of license plates as they move into a camera’s view. There is a WSDOT network router installed near an SDOT network router in the Seattle Municipal Tower. The two networks are separated by an SDOT-managed firewall that is responsible for filtering the data traffic. The LPR images are processed into raw data within the camera itself and are put through SDOT’s firewall that reports the license plate number to WSDOT with a 1) time stamp, 2) plate number, 3) LPR camera channel, and 4) station (intersection) identifier. SDOT’s firewall also translates each LPR camera’s IP address so it can be sent to WSDOT. SDOT does not validate the WSDOT endpoint,³² and the data is not encrypted as there is a dedicated, secure fiber optic network between SDOT and WSDOT.

WSDOT’s central computer (Windows server) downloads SDOT LPR plate reads every 20 seconds. WSDOT said their processing system was developed by one programmer at WSDOT, and that the system only processes the license plate numbers and time stamps.

According to WSDOT, the license plate data is converted from memory into identifiers that are written to disk in temporary files and that all temporary files greater than seven days are auto-purged at 4:00 AM every morning. The files do not contain any humanly readable information because the license

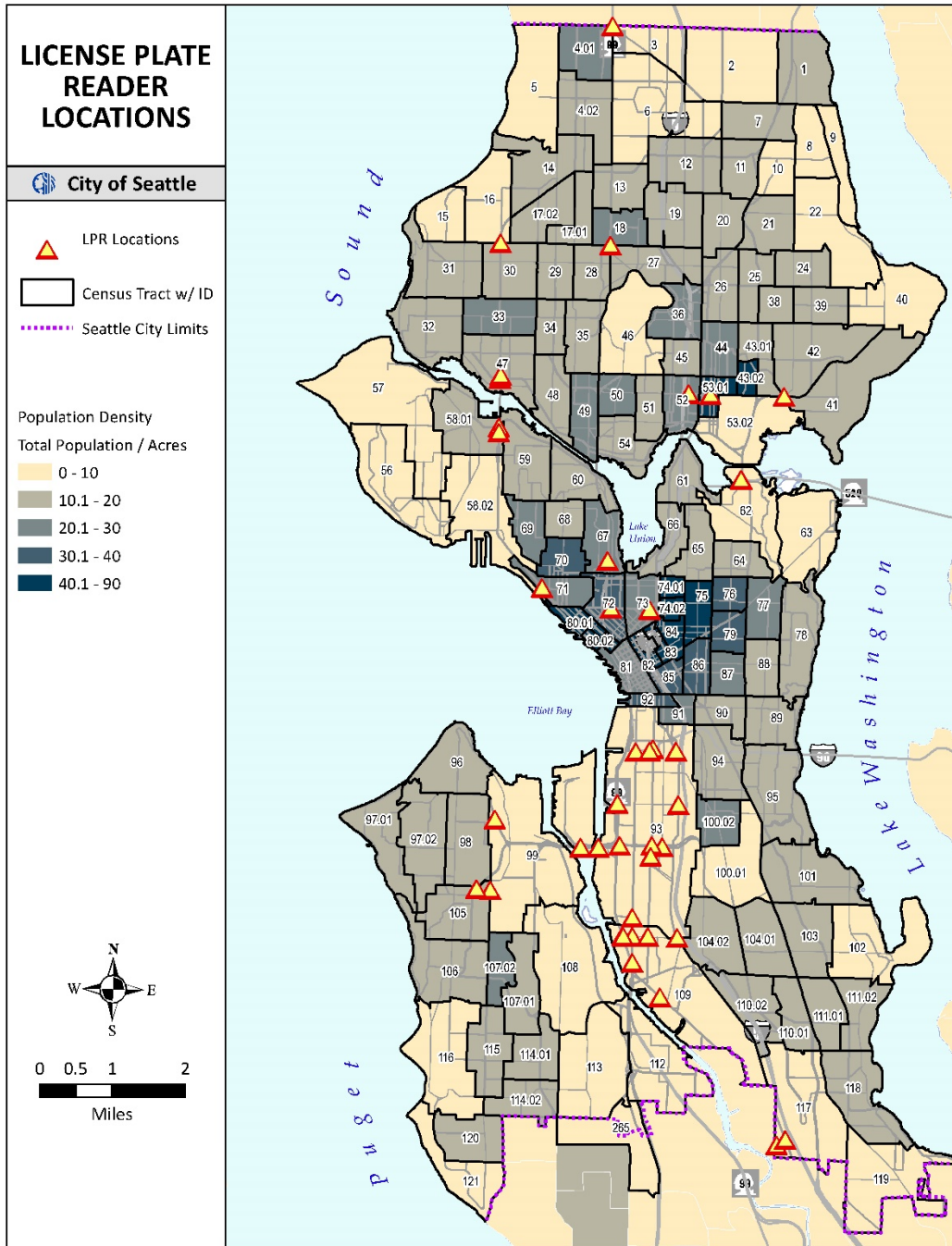
³² An endpoint is any device that is physically an end point on a network. Source: [Webroot](#)

plates are converted into an anonymized index and the time stamps are written in binary code. WSDOT stated that they do not have a tool written to unpack the data in the files. WSDOT also informed us that if someone wanted to get license plate data, they would need to obtain the files within seven days and would have to reverse engineer the WSDOT program that writes the files, and the code is not in the public domain. Also, the files are on a secured server on a private non-routable network that is protected by firewalls. Five WSDOT personnel have access to the files and only one WSDOT employee knows the file format.

SDOT told us that travel time is calculated based on an average of a minimum of five license plates that are captured as matches between points A and B; SDOT receives travel time information back via the WSDOT-hosted Application Public Interface (API). The information is received by custom built SDOT software, which in turn feeds the relevant data into SDOT's Cameleon Intelligent Transportation Systems (ITS) sign control software. Cameleon ITS then sends the travel time information to SDOT Dynamic Message Signs (DMS). SDOT also provides travel time information from WSDOT on SDOT's [Traveler Information Map](#) website.

APPENDIX G

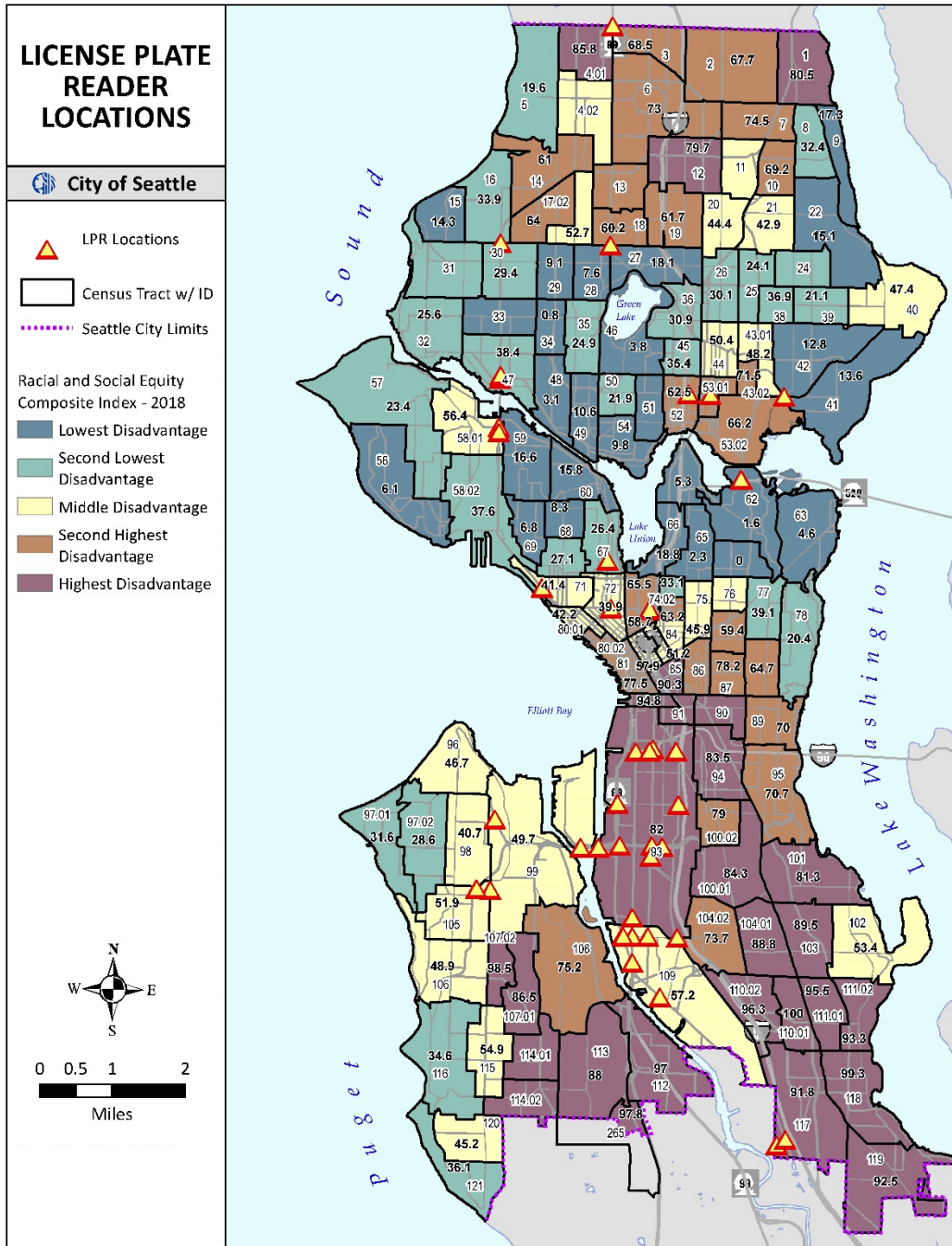
Population Density



Source: Seattle Department of Transportation and Department of Information Technology GIS Products and Services.
Note: Some LPRs may appear overlapping.

APPENDIX H

Race and Social Equity Composite Index



Source: Seattle Department of Transportation and Department of Information Technology GIS Products and Services.
 Note: Some LPRs may appear overlapping.

APPENDIX I

Acknowledgements

The Office of City Auditor would like to thank staff from the following City departments for their cooperation on this audit and responsiveness to requests for information, documents, and data:

- SDOT Transportation Operations Center (TOC)
- SDOT Finance and Administration Division
- SDOT Project Development Division
- Legislative City Clerk, Information Technology
- Finance and Administrative Services, Customer Services Division
- Seattle Information Technology Department, GIS Products and Services
- Seattle Information Technology Department, Privacy Team
- Seattle Information Technology Department, Cybersecurity/Risk Management
- Office of Planning & Community Development, Citywide Initiatives

We would like to thank the Seattle Information Technology Department, GIS Products and Services for providing GIS mapping and demographic analysis.

- We would also like to thank the following parties from outside the City of Seattle: [Intelligent Transportation Systems Operations](#) staff from the Washington State Department of Transportation
- ACLU-Washington
- A citizen advocate for surveillance technology concerns

APPENDIX J

Seattle Office of City Auditor Mission, Background, and Quality Assurance

Our Mission:

To help the City of Seattle achieve honest, efficient management and full accountability throughout City government. We serve the public interest by providing the City Council, Mayor and City department heads with accurate information, unbiased analysis, and objective recommendations on how best to use public resources in support of the well-being of Seattle residents.

Background:

Seattle voters established our office by a 1991 amendment to the City Charter. The office is an independent department within the legislative branch of City government. The City Auditor reports to the City Council and has a four-year term to ensure her/his independence in deciding what work the office should perform and reporting the results of this work. The Office of City Auditor conducts performance audits and non-audit projects covering City of Seattle programs, departments, grants, and contracts. The City Auditor's goal is to ensure that the City of Seattle is run as effectively, efficiently, and equitably as possible in compliance with applicable laws and regulations.

How We Ensure Quality:

The office's work is performed in accordance with the Government Auditing Standards issued by the Comptroller General of the United States. These standards provide guidelines for audit planning, fieldwork, quality control systems, staff training, and reporting of results. In addition, the standards require that external auditors periodically review our office's policies, procedures, and activities to ensure that we adhere to these professional standards.

Seattle Office of City Auditor
700 Fifth Avenue, Suite 2410
Seattle WA 98124-4729
Ph: 206-233-3801
www.seattle.gov/cityauditor