POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

2018 Privacy Impact Assessment

PAY STATION REPLACEMENT PROJECT

SEATTLE DEPARTMENT OF TRANSPORTATION (SDOT)

08.27.2018

Seattle
Information Technology

CONTENTS

PRIVACY IMPACT ASSESSMENT OVERVIEW

WHAT IS A PRIVACY IMPACT ASSESSMENT?

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

WHEN IS A PRIVACY IMPACT ASSESSMENT REQUIRED?

A PIA may be required in two circumstances.

- The first is when a project, technology, or other review has been flagged as having a high privacy risk.
- The second is when a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

HOW TO COMPLETE THIS DOCUMENT?

As department staff complete the document, they should keep the following in mind.

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

1.0 ABSTRACT

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

This 1-3 sentence explanation should include the name of the project/ technology/ program/ application/ pilot (hereinafter referred to as "project/technology"). It should also include a brief description of the project/technology and its function.

SDOT's Parking Pay Station Replacement Project's objective is to replace aging on-street paid parking equipment, originally installed in the mid-2000s and at the end of useful life, with pay stations that support SDOT's data-driven, demand-based rate setting program, provide a better customer experience, and are more reliable, with pay stations with improved communications connectivity which are future-proofed against technological and regulatory changes. SDOT recently completed the replacement of over 1,500 pay stations with IPS Group, Inc., multi-space kiosks. The final phase of the project will convert the payment process from a pay and display to pay by license plate mode, where parkers will enter their license plate into an alphanumeric keypad at the kiosk rather than return to their car with a sticky receipt for the window.

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

This 1-3 sentence explanation should include the reasons that caused the project/technology to be identified as "privacy sensitive" in the Privacy Threshold Analysis form, such as the project/technology collection of personal information, or that the project/technology meets the criteria for surveillance.

For the reasons stated above, SDOT replaced the aging pay stations with newer technology. The final phase of the project transitions the payment methodology from pay and display to pay by plate. This project has been identified as "privacy sensitive" due to the media attention that has been generated by the announcement of this change. SDOT has developed a public education campaign to inform the parking public about the change, so the media visibility will continue through 2018 as we transition from pay and display to pay by plate, block by block throughout the paid parking areas of the city. The Privacy Impact Assessment will aid in transparency and help any concerned user understand what and how their information is handled and used. The project previously went through a surveillance review in which it was deemed that this technology is not considered surveillance.

2.0 PROJECT / TECHNOLOGY OVERVIEW

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

2.1 Describe the benefits of the project/technology.

The project replaced aging pay stations with newer, more flexible, and user-friendly pay stations. This includes the following benefits:

1. Improved user interface
2. Improved communications reliability
3. Faster credit card transactions
4. Swipe-style credit card readers to allow users to maintain control of their cards
5. New back-office software to improve departmental ability to detect problems remotely and fix them faster
6. Enable "time of day" pricing to allow for lower rates at off-peak times, and higher rates when necessary to more effectively manager parking demand and access
7. Pay by license plate allows users to park, pay and be on their way with no need to return to their car enabling greater efficiency and less possibility for error for users and parking enforcement

2.2 Provide any data or research demonstrating anticipated benefits.

The new IPS pay stations have delivered on all elements listed above.

There are many reasons for the transition to pay by plate payment. Other cities have determined that pay by plate provides improved customer benefits and enforcement efficiencies. Plate-based systems are used by every mobile phone parking payment system, including Seattle's, and growing in use throughout the country and world. Seattle is currently at 30% mobile phone payment adoption. Many cities are migrating to pay by plate systems to allow for efficient enforcement where all payment data is in one back office. Many cities have already migrated to pay by plate, including Calgary, Denver, Pittsburgh, Miami, Houston, and Portland.

2.3 Describe the technology involved.

Pay stations and their supporting systems have many different technological components. For example, there are over 160 different software programing configurations currently deployed on the streets of Seattle, regulating the various combinations of hours of payment, maximum time, morning/afternoon/evening rates, pre-payment functionality, and peak hour parking restrictions. Printer firmware, modem firmware, solar board programming, e-locks, RFID programming, and many other technologies are used. For purposes of this document, the focus is on the communications technology. Pay stations use cellular modems for communications. These communication technologies provide connectivity for online credit card transactions so that transaction and parking data may be sent to the vendor back office through digital interfaces. Paid parking session data is sent to the parking enforcement vendor's system and handhelds to allow for remote maintenance monitoring by pay station technicians. Our vendor, IPS Group, Inc., is a leader in PCI (Payment Card Industry) compliance, attaining Level 1 PA-DSS and PCI-DSS (meaning they are certified at the highest levels of data security for both the specific pay station equipment and the platform/system on which it runs). Level 1 requires data be held consistent with the very highest security standards, including encryption, penetration testing, and server security. These systems and protocols protect credit card data and license plate data. Our vendor will never share nor sell personal data to any third party; it is used for the sole purpose of fulfilling their obligations under their contract with the City to process on-street paid parking transactions. Since installing pay stations in 2004 that have accepted debit/credit cards, and processing about 11 million transactions per year, the City has not experienced a data breach. IPS Group, Inc. has adopted the privacy principals of the GDPR (General Data Protection Regulation) which are strict data privacy protection regulations that went into effect in the EU May 25, 2018, and have been called the most important changes to data privacy in 20 years.

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

SDOT's mission is "To deliver a high-quality transportation system for Seattle." This project supports that overall mission by replacing aging systems with newer, more user-friendly technology that is more reliable. This project also supports SDOTs Performance-Based Parking Pricing Program with a wide range of recommended pricing strategies for optimizing paid parking throughout the city to provide reliable access to customers and visitors.

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

SDOT has contracted with IPS Group, Inc. for the system and implementation. As an international company offering a variety of paid parking and enforcement technologies, IPS Group, Inc. are PCI-DSS and PA-DSS Level 1 certified providers and meet GDPR (European) Privacy regulations.

3.0 USE GOVERNANCE

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

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

This is not applicable, as this is a pay station payment system for public use street parking and the pay stations are permanently installed on the streets.

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

For example, the purposes of a criminal investigation are supported by reasonable suspicion.

This is not applicable, as this is a pay station payment system for public use street parking.

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

Include links to all policies referenced.

IPS Group, Inc. is a PCI-DSS and PA-DSS Level 1 certified provider and meets GDPR Privacy regulations. For more details about IPS Group, Inc.'s privacy and compliance policies please consult the following:

- Privacy Policy: https://www.ipsgroupinc.com/privacy-policy-update/
- PCI Compliance: https://www.ipsgroupinc.com/resources/pci-certifications/

IPS Group, Inc., contracts with certified third-party auditors for their annual PCI compliance reports. Per City requirements, Seattle IT's PCI Compliance Manager holds a copy of IPS Group, Inc.'s current Attestation of Compliance (AOC) and ensures they maintain their Level 1 standing.

All SDOT parking staff are trained in PCI Security Standards and Skimmer Detection. Standard Operating Procedures instruct staff in responsibilities. Modems and card readers are kept in secure facilities where only authorized people are allowed entry. Skimmer checks are performed according to schedule.

4.0 DATA COLLECTION AND USE

Provide information about the policies and practices around the collection and use of the data collected.

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

This is not applicable, as this is a pay station payment system for public use street parking and collects and uses only the information that is provided by the user to pay for parking.

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

This is not applicable, as this is a pay station payment system for public use street parking and collects and uses only the information that is provided by the user to pay for parking. We cannot collect anything that is not submitted by the user at the pay station at the time of transaction.

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

This is a deployed pay station system for street parking and is used by members of the public to pay for parking according to posted pay schedules and rates.

4.4 How often will the technology be in operation?

Pay station kiosks are in operation daily, available 24x7, and in effect as regulated and posted regarding holidays and required hours.

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

Pay station kiosks are permanent installations throughout the city of Seattle.

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

Pay station kiosks are well-signed and provide instructions for use and directions for methods of fee payment. The user interface guides the user and provides information throughout the transaction, from start to conclusion. SDOT also maintains information online here: www.seattle.gov/parking

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

Please do not include staff names; roles or functions only.

The City of Seattle is not collecting or storing any personally identifiable information. Our vendor stores data consistent with PCI Level 1 standards, consistent with GDPR Privacy regulations. Only authorized personnel from SDOT and Seattle Police Department (SPD) have access. SPD Parking Enforcement can view the paid status of vehicle license plates via their enforcement devices for issuing citations for non-payment; management can access data to confirm that citations were issued appropriately and to confirm systems are operating properly. SDOT management and maintenance have access to the system for limited purposes (refunding double payments, verifying payment, providing copies of receipts) on a customer request basis; management can access data to confirm systems are operating properly.

Non-personally identifiable data of pay station and pay by phone transactions, as well as parking curbspace asset management data, are publicly available through Seattle's open data program.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols. Please link memorandums of agreement, contracts, etc. that are applicable.

See answer to 4.7. The link to the contract documents appears below: http://web6.seattle.gov/FAS/SummitPan/R296/R296.ResultAttachments.aspx?CNTRCT_ID=0000003155&NAME1=IPS+GROUP+INC&SortOnReturn=SortOnReturn=vwstgrdvPoListSortExp%253d%2526vwstgrdvPoListSortDir%253d0

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

SPD Parking Enforcement has access to certain information for parking enforcement purposes. Officers in the field see in their handheld devices the license plate numbers that are currently in paid status. SPD and SDOT management and maintenance have access to the system for limited purposes (refunding double payments, verifying payment, providing copies of receipts) on a customer request basis. SPD and SDOT technical and management staff can view transaction history in the back office to confirm systems are operating properly.

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

Data is held by the City's vendor, IPS Group, Inc., consistent with PCI Level 1 standards and GDPR Privacy regulations. Only authorized people are provided with password protected accounts to access the back office Data Management System (DMS); transaction data is read-only and cannot be modified by City personnel. Data on the paid status of a vehicle is transmitted through API (Application Programming Interface), used to securely send data to the Parking Enforcement system.

5.0 DATA STORAGE, RETENTION AND DELETION

5.1 How will data be securely stored?

Data is stored by the City's vendor and is consistent with PCI Level 1 standards and GDPR Privacy regulations.

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

IPS Group, Inc. will retain the data per City policy/request, will truncate personally identifiable data per City policy/request and will comply with City requirements to confirm deletion of data.

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

This is not applicable, as this is a pay station payment system for public use street parking and collects and uses only the information that is provided by the user to pay for parking. We cannot collect anything that is not submitted by the user at the pay station at the time of transaction.

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

The unit responsible for ensuring compliance is the Parking Project's Lead in SDOT's Transit & Mobility, Parking and Access Section.

6.0 DATA SHARING AND ACCURACY

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

The Seattle Police Department's Parking Enforcement Division receives appropriate data to fulfill their enforcement mission. SDOT shares parking transaction data for posting on the City of Seattle's open data portal. There is no personally identifiable data in the parking transaction records (e.g., no license plate, no credit card, etc.).

6.2 Why is data sharing necessary?

SPD requires information for parking enforcement purposes and the City of Seattle Open Data Portal provides de-identified information for research and entrepreneurial purposes.

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

Yes ☐ No ☒

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

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies? Please describe the process for reviewing and updating data sharing agreements.

The parking transaction data available on data.seattle.gov does not have any restrictions on usage. SDOT staff encourage vendors, researchers, and others interested in parking information to contact us to discuss how they are using parking data, but there is not an obligation to do so under the City's open data program.

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

The data comes from the user entering their license plate, inserting card or coin, and selecting the amount of paid parking time desired. If the user enters the license plate number incorrectly, they risk getting a parking citation for non-payment, though enforcement officers can use discretion if it appears to be a mistake. The transaction record data is created in the back office by the action of paying for parking and is not editable.

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

Transaction records are not editable.

7.0 LEGAL OBLIGATIONS, RISKS AND COMPLIANCE

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

Relevant Seattle Municipal Code sections:
11.16.300 Traffic Engineer—Authority—Parking: authorizes the establishment of paid parking areas
11.31.121 Monetary penalties—Parking infractions: establishes the fines for non-payment
11.76.005 Proper payment: requires users to provide license plate or space number

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

For example, police department responses may include references to the Seattle Police Manual.

All SDOT parking staff are required to take the privacy training course titled, "Privacy and Information Security Awareness."

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

Please work with the Privacy Team to identify the specific risks and mitigations applicable to this project / technology.

Risk: data breach. Mitigation: the City's vendor is certified PCI Level 1 and is compliant with GDPR Privacy regulations.

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

Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected, that is not explained in the initial notification.

License plate and credit card data are personally identifiable, and collection of this information can cause concern about personal privacy. The City, however, does not store any personally identifiable data. Our vendor stores this data under the tight security of PCI and GDPR Privacy regulations. Only authorized personnel from SDOT and SPD have access. SPD Parking Enforcement can view the paid status of vehicle license plates via their enforcement devices for issuing citations for non-payment; management can access data to confirm that citations were issued appropriately and to confirm systems are operating properly. SDOT management and maintenance have access to the system for limited purposes (refunding double payments, verifying payment, providing copies of receipts) on a customer request basis; management can access data to confirm systems are operating properly.

8.0 MONITORING AND ENFORCEMENT

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

We do not believe our vendor would ever be required to disclose personally identifiable data and it would be against their policy to do so. Non-personally identifiable data is available to everyone on the City's Open data portal.

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

IPS Group, Inc. contracts with certified third-party auditors for their annual PCI compliance reports. Per City requirements, Seattle IT's PCI Compliance Manager holds a copy of IPS Group, Inc.'s current Attestation of Compliance (AOC) and ensures they maintain their Level 1 standing. These certifications are subject to audits by independent third parties.