2018 Privacy Impact Assessment

BIKE SHARE PROGRAM

DEPARTMENT OF TRANSPORTATION

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 Free-Floating Bike Share Program permits **private vendors to deploy bicycles** and related personal mobility devices on public right-of-way for rental. The devices are equipped with a GPS tracker that the company and City will use to track the devices' location and manage use of the public right-of-way. SDOT will require the vendor to **share the GPS location data** and other specific attributes either directly with SDOT or with an independent data analyst of SDOT's choosing. Since SDOT has not identified an independent data analyst, this PIA addresses the privacy impacts of data sharing directly with SDOT.

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.

After completing a Privacy Threshold Analysis, the Privacy office informed us that while the data we collect is considered "low privacy harm risk" a PIA is required to ensure maximum transparency to the public and service users about the collection and use of data. The program will collect location information on the vendor's devices, including the location of available devices and the origins, destinations, and waypoints of trips as measured by the device's GPS unit or the location services on a rider's phone, if enabled. SDOT will not collect personally identifiable data.

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 Free-Floating Bike Share Program permits private vendors to deploy bicycles and related personal mobility devices on public right-of-way for rental. Riders can find the nearest device, rent it, ride it to their destination, and leave the device for the next rider. Most riders locate and rent devices with a smartphone app, but we require vendors to offer at least one option for riders who have neither a charge card or a smartphone. (All vendors propose using PayNearMe as a low-barrier rental option.)

During the pilot phase of the program, we saw 1.4 million rides in 11 months. Pronto, Seattle's previous bike sharing program, recorded 280,000 rides over 30 months.

The location data we collect on trips and deployed devices will provide several benefits to the City:

- **The data are critical to managing the program and evaluating vendor compliance.** Based on our pilot data and City policies, we set numerous compliance standards for vendors to follow (e.g. minimum and maximum number of devices deployed in the City; the distribution of those devices across certain neighborhoods). We will use the collected available-device data to measure the vendor's compliance daily.
- **With deployed-device data, we can evaluate crowding and parking impacts** on the right-of-way (though the data is not granular enough to know whether a device is parked correctly without physically traveling to the device for an inspection). We can also evaluate how the vendors' distribution of devices may create advantages or disadvantages in certain neighborhoods, such as evidence of "redlining" (or avoiding deployment of devices in certain places). We are committed to an equitable bike share program, so evidence of inequity is crucial to evaluating system performance.
- Trip data (starts, ends, and waypoints) will allow us to **evaluate cycling use** of our rights-of-way, including determining **which corridors riders prefer or avoid**. We can link this information to traffic, weather, and elevation data for further insights. The data can help SDOT target cycling infrastructure investments and evaluate intersection level of service for cyclists.
- Trip data also **helps us determine how well the system is performing** and how it has changed the mobility characteristics of different parts of the City.

2.2 Provide any data or research demonstrating anticipated benefits.

During the pilot (July 2017 to present), we collected trip and deployed device data through the University of Washington's Transportation Data Collaborative. The data they collected allowed us to develop our pilot evaluation, released in August 2018 (available at https://www.seattle.gov/Documents/Departments/SDOT/BikeProgram/2017BikeShareEvaluationReport.pdf). We gained valuable insights into the use of and demand for device sharing across the City and over time, as well as basic data on common trip types and corridors.

2.3 Describe the technology involved.

Each shared device (usually a bicycle) is equipped with a **GPS tracking unit**. That tracking device transmits the device's location (upon specified events and at specified intervals) to the vendor, who collects the records. The vendor then reports the data to SDOT through an **API or table** for analysis and compliance evaluation.

Some vendors may supplement or substitute the on-bike GPS data with GPS data collected from the rider's phone. The vendor's ability to collect phone location data depends on the rider's location services settings. We do not regulate whether the vendor may collect other data that is not reported to SDOT (e.g. a person's location whenever they open the app).

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

SDOT's mission is to **develop a high-quality transportation system** for Seattle. The Free-Floating Bike Share Program provides an additional mobility option for people in Seattle. The collected data helps us better manage both the program and the right-of-way the program occupies. Particularly as the city center undergoes major capital projects, we need to understand how people are using the program and how it can fill mobility gaps. Data on the devices' parking patterns is particularly important for maintaining safe, wheelchair-accessible sidewalks and curb ramps.

Collection and use of the data is also consistent with SDOT's **New Mobility Playbook**. For emerging mobility systems, good information is just as important as good infrastructure. In this instance, collecting some of the data vendors already collect will provide us the information we need to maximize the public benefits of this service while mitigating negative impacts.

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

The bike share Program team consists of the Bike Share Program Manager and one additional staff member. The bike share team is part of SDOT's New Mobility Team, in turn a part of the Transit and Mobility Division. The bike share team works with SDOT's Data Science team and Street Use Division, as well as staff throughout SDOT, at IT and other departments, and at other cities and agencies.

The data's anticipated chain of custody is as follows:

- **The vendors** will physically deploy and maintain the tracked devices and their tracking components. The vendor's tracking devices report the data to the vendor, who will then **submit the data to the City**.
- **Data will be stored for SDOT in** a data warehouse that the IT Department is building.
- SDOT's **Data Science team** will process and clean the data. Some basic processing may be built into the data warehouse system.
- The **Program team** will use the processed data to evaluate the vendor's compliance with the permit requirements, including data integrity. A set of **compliance queries will run automatically** on the data as it comes in. The Program team may also query the data to understand the system's overall performance and for program and infrastructure planning purposes.
- Data analytics may be displayed for the Program team using Tableau or another **data visualization** platform.
- **Other SDOT teams** may also use this performance data to help the City better understand community needs and improve the efficiency, effectiveness, and equity of our service delivery. We may tailor the data shared to its use case in each instance.
- SDOT may publish the deployed-device data for **public use** through coordinated street furniture, transit screens, or other means.
- The data may be subject to **public disclosure**.
- We anticipate retaining some elements of the data indefinitely for **research and planning purposes**. We may simplify retained data by aggregating it or deleting unnecessary fields after we have processed the data. We will follow city and state requirements for records retention.

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.

IT and SDOT's Data Science team will manage and store the data on behalf of the Program team. The Data Science team may establish one or more data portals to permit access to different entities (the Program team, infrastructure planning teams, researchers, public information screens). Teams or other entities who want to use the data must notify the Program and Data Science teams to coordinate the use.

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.

Data will only be collected from vendors who have applied for and been selected to receive a Street Use permit. **The vendors must agree to provide the data as a condition of being approved** for the permit. The vendors must also agree to **notify riders of the data the vendor collects and shares**.

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.

SDOT's new permit requirements (available at http://www.seattle.gov/Documents/Departments/SDOT/BikeProgram/SeattleBikeSharePermitRequirements2018.pdf) describe the data collection and sharing policies that vendors must follow.

Requirement DS1 describes the data collection and sharing requirements discussed in this Privacy Impact Assessment.

Appendix E.1 and E.2(a) describe the data fields we will collect under this PIA. (We will not use the E.2(b) table for data submitted directly to SDOT.)

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.

The data we collect is generated from the GPS tracker mounted on each bicycle or other device. Currently, some vendors use mobile phone GPS to supplement or replace the on-device GPS during trips; new devices deployed beginning in March 2019 must be capable of relying solely on the on-device GPS (to limit trips dropped because riders used their phones during the ride). Devices that still rely on mobile phone GPS will still be permitted to operate through the rest of the permit year.

We will collect **X,Y coordinate data:**

- **for each deployed device** that is not being rented (when the device is deployed, when it is removed from deployment, and for the duration of deployment as frequently as every 30 minutes); and
- **for each trip taken** on a device (at trip start, trip end, and throughout the trip as frequently as every three minutes).

For data analysis, we may compare and synthesize the collected data with traffic counters, demographic data, weather data, and GIS data (elevation, land use, etc.).

If the vendor collects data through the rider's mobile phone, then the vendor may use the phone's GPS to obtain location data. Use of the phone's location data depends on the rider's location services settings, but the vendors' apps require location data when they are in use to show the nearest devices to a rider. The vendor may record additional rider location data that SDOT does not ask for, such as location data whenever the rider opens the app to look for a device (regardless of whether the rider ultimately starts a trip). Some incoming vendors also offer other transportation services (such as TNC/ridehailing) and may collect additional information from users for those services. At least one vendor has committed to providing aggregate mode-shift data describing how its existing ridehailing users transition to bike sharing.

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

SDOT will manage vendors' data collection and integrity under the permit requirements. As part of their permit applications, the vendors provided information on their data collection and integrity structure. The vendors' authorized agents completed a notarized signature page indicating their agreement to comply with the permit requirements. The vendors are issued a permit based in part on these representations; if the vendor does not perform as required, SDOT may revoke their permit or take other enforcement action as described in Requirements CE1, CE2, and CE5.

After reviewing the vendors' applications and discussing their data collection plans, we have obtained each vendor's written agreement (in addition to the notarized signature page) that they will comply with our data requirements. We will not directly observe the vendors collect data during the permit, but we can take corrective action if concerns about inadvertent or improper collection arise in the data the vendor submits to SDOT.

SDOT may accept or reject data it receives. We will reject data that includes rider identification information.

Though vendors are required to submit data relating only to trips and devices in or within 1000 feet of Seattle, some vendors may elect to submit wider regional data. We believe the regional data will provide added value to the required data, so we do not consider it an improper collection.

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?

- **The vendor "deploys" the devices** on which the GPS trackers are mounted and makes agreements with the riders for use of the devices and collection of the data.
- Members of the **public will ride** and use the devices.
- **SDOT manages the program**; no vendor may deploy a device unless the Program Manager has approved it and unless it meets certain equipment requirements. The permit requirements also **regulate the number and distribution of devices** (which we measure with the collected data).

4.4 How often will the technology be in operation?

We expect GPS trackers to be active on **10,000 to 20,000 devices** at a time by November 1, 2018. By March 2019, we may have 20,000 or more active devices deployed at a time. The individual devices will change due to fleet attrition or movement out of the City, but we require the vendors to maintain this fleet size as measured daily. The number of devices (and their allocation among vendors) may change over the permit year due to enforcement action, reallocation, and fleet size changes.

The devices will **collect deployed-device data whenever deployed**. When a rider rents the device, trip records will be generated from the device or the rider's phone GPS.

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

The devices are temporary. All deploying vendors must have a permit, which may be renewed upon successful application. **SDOT may revoke the permit at any time** and require the vendor to remove its devices from the public right-of-way.

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?

The bicycles or other devices collect the data. We require the vendor to place its trade name and contact information on the device. The tracking component is not prominently marked on the devices, but **riders have notice that the device's location is tracked** because 1) we require the vendor to notify riders of the data the devices collect, and 2) most riders locate the device by traveling to the location its GPS tracking unit reports in the smartphone app.

If the vendor collects trip data from the rider's phone, the vendor obtains permission to do so consistent with the requirements governing their phone's operating environment.

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

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

The SDOT Data Science Team and the Program Team will have frequent access to the collected data. Other teams at SDOT may obtain access to the data on request. We may publish deployed-device data to transit screens. The data may be publicly disclosable.

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.

The protocols governing SDOT's relationship with the vendors are contained in the permit requirements. SDOT has reserved the flexibility to contract with an independent data analyst, but SDOT has no plans at this time to provide the data it collects from the vendors to another entity.

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

We would make the data available for research and planning purposes. In consultation with IT, we are evaluating how data provided to an individual requestor can be tailored to their needs and minimize the release of raw data where possible. Others may access the data through public records request.

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.)?

Most data access within SDOT will occur through APIs. The Data Science Team will provide the API keys that an authorized person needs to access the API. SDOT maintains records of public disclosure requests.

The data warehouse is now under construction, and we will work with IT to develop appropriate security, access control, and audit trail procedures. We will also explore how data encryption may improve security even for data that is publicly disclosed.

5.0 DATA STORAGE, RETENTION AND DELETION

5.1 How will data be securely stored?

IT is now building an SDOT Mobility Data Warehouse in which bike share data will be stored. The warehouse may grow to include other mobility data.

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

The Data Science Team can make the data available for this purpose on request.

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

The data warehouse will pull specific data fields from each vendor and will not pull more fields than those specified. The Data Science Team may reject or destroy improperly collected data. We do not anticipate that the vendors will volunteer any sensitive data that SDOT has not required them to share.

If a vendor elects to share deployed-device or trip data over a larger geographic area than we require (e.g. all of King County), we will not consider the data to be improperly collected for this reason alone. We may retain the data for its probative value in showing cycling activity to and from Seattle.

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

We are still determining our internal data organization and storage plan.

6.0 DATA SHARING AND ACCURACY

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

The vendors collect the data and share it with SDOT. Outside of SDOT, we may share data with other departments such as the Seattle Department of Parks and Recreation. We may contract with other entities to provide data services that will support our in-house management of the data. Vendors may require a rider to agree to terms of service that provide for data collection and sharing with other third parties outside the scope of City use or permit regulations.

6.2 Why is data sharing necessary?

These devices are deployed on public right-of-way, which SDOT has a duty to maintain and regulate. Without data sharing, SDOT has no access to the location data that vendors collect. SDOT needs vendors to share the data **so that we know where devices are and how they are being used**. We need this information to successfully manage the program and its impacts.

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.

We are still developing procedures for data use, but we anticipate that non-City data use would be restricted to applicable public disclosure and to providing either aggregated data or the opportunity to query raw data to non-City entities pursuant to a contract or MOU. We may release some of the data for public use, such as deployed-device data for transit screens (so people can see if devices are nearby).

6.4 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?

Yes ☒ No ☐

6.4.1 Please describe the process for reviewing and updating data sharing agreements.

We are still developing procedures for data use, but we may release aggregated data through Seattle's open data portal. The Bike Share Program Manager, in consultation with the Data Science Team, would evaluate requests for additional data.

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

The Data Science team will check the data's integrity against itself in several ways:

- Check timestamps and device IDs, to ensure data is reported for each device at the **required frequency**;
- Check trip data to ensure **trips are not dropped**; and
- Compare locations reported by trip data and deployed-device data to ensure internal consistency.
- The Program Team or its designee will also **ground-truth** the data's integrity through compliance auditing. This will include physically inspecting deployed devices and then checking to ensure they appear as expected in the data the vendor reports to SDOT.

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

SDOT will not accept trip data that is linked to rider ID or other personally identifying information. Since the data will not be individually identified, there are no procedures for an individual to find data specifically about them.

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?

SDOT issues the street use permits for this program under its authority in **SMC titles** 11 **and** 15. We will also publish permit requirements to govern the vendor-SDOT data-sharing relationship.

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.

Regular privacy and security training will be provided to all City personnel.

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.

The primary privacy risk is that trip location data could be personally identifiable. We have committed to several mitigation measures:

- We **will not collect personally identifiable information** for individual riders (name, email, etc.).
- We will not capture addresses, only coordinates.
- We will not collect rider ID for data provided directly to SDOT.
- We will not link ride data to survey responses or demographic data.

Without a rider ID, there is no information linking trips to individuals. Individual ridership patterns may not be determined from information that may be disclosed in a public records request or open data set.

We believe these steps should greatly reduce the risk that an individual may be personally identified using GPS coordinate bike share data alone.

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.

Since the data may be publicly disclosable, **a third party can obtain the data.** They could in turn analyze and publicize the data, including records of individual trips (though not who took the trip). We anticipate mainly research interest involving the aggregation of trip and deployment data.

SDOT may work with third-party data analysts (independent or not) to manage and analyze the data. Since the vendor collects the data, we have no control over its use or distribution of the data outside of its agreements with SDOT and its designees. Riders sign agreements with the vendors to rent the devices that include details about terms of use, data sharing and other aspects of the vendor's data management policies.

The Privacy Threshold Analysis feedback noted that **the program should not look like a City service**. As in the pilot, the devices will carry the vendors' trade name and branding, and the vendor bears primary responsibility for fleet management and rider education.

We have taken the following **mitigation steps**:

- The permit requirements disclose that SDOT's designees may access and use the data.
- The vendor must disclose its data sharing practices to riders.
- The vendor must provide its user agreements to SDOT for review to ensure that the data collection disclosure is sufficient.
- We will have a 6-month check-in with the City Privacy team to review and identify any areas of concern. We can modify our data collection standards as needed to mitigate concerns that arise.

8.0 MONITORING AND ENFORCEMENT

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

SDOT has a public disclosure team that maintains records of disclosure requests under the Public Records Act. The Program and Data Science teams will also maintain records for disclosures, including copies of MOAs, contracts, and contact information. The data warehouse is still being developed, but it may automatically retain records of access and data queries.

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.

With respect to the devices and their data collection accuracy, the Program team will review fleet data (trip and deployed-device data) in conjunction with data obtained through a fleet audit (internal, third-party, or a mix).

We are still developing our data warehouse, but IT and/or our Data Privacy Team can periodically self-audit the security of the warehouse and its data.