POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

City of Seattle Privacy Impact Assessment

DOWNTOWN PARKS PEDESTRIAN COUNTERS PROJECT

Owner: Parks & Recreation Department

Date: 9/28/2017

12.7.2017

Seattle
Information Technology

CONTENTS

PURPOSE OF PIA

A Privacy Impact Assessment is designed to outline the anticipated privacy impacts from a City project/program or project/program update that collects, manages, retains or shares personal information from the public. The PIA will provide project/program details that will be used to determine how privacy impacts may be mitigated or reduced in accordance with the City of Seattle Privacy Principles and Privacy Statement.

ABSTRACT

Please provide a brief abstract. *The abstract is the single paragraph that will be used to describe the project and* ***will be published on the Privacy Program website.*** *It should be a minimum of three sentences and a maximum of four, and use the following format:*

- *The first sentence should include the name of the project, technology, pilot, or project/program (hereinafter referred to as "project/program").*
- *The second sentence should be a brief description of the project/program and its function.*
- *The third sentence should explain the reason the project/program is being created or updated and why the PIA is required. This sentence should include the reasons that caused the project/program to be identified as a "privacy sensitive system" in the Privacy Intake Form, such as the project/program requiring personal information, or the technology being considered privacy sensitive.*

The Downtown Parks Pedestrian Counters project will be managed by the Downtown Seattle Association (DSA), under a forthcoming agreement with the City. DSA will contract with a vendor (MotionLoft) to install sensor devices in downtown parks which will collect park-use data for performance measures and planning in regard to activation and improvement projects. The sensors are cameras that capture an image to determine pedestrian volume and direction traveling. The captured video frame is used to identify the image as pedestrian, vehicle, or animal. The count, date, time, direction, weather, temperature, precipitation, latitude, longitude, and events (metadata) are sent over an encrypted connection and stored in the Amazon Web Services (AWS) - GovCloud.

PROJECT/PROGRAM OVERVIEW

Please provide an overview of the project/program. *The overview provides the context and background necessary to understand the project/program's purpose and mission and the justification for operating a privacy sensitive project/program. Include the following:*

- *Describe the purpose of the system, technology, pilot or project/program; the name of the department that owns or is funding the project/program and how it the project/program relates to the department's mission;*
- *Describe how the project/program collects and uses personal information, including a typical transaction that details the life cycle from collection to disposal of the information;*
- *Describe any routine information sharing conducted by the project/program both within City of Seattle departments and with external partners. Describe how such external sharing is designed with the original collection of the information.*

- *Identify any major potential privacy risks identified and briefly discuss overall privacy impact of the project/program on individuals*
- *Identify the technology used and provide a brief description of how it collects information for the project/program.*

Purpose

Under a 5-year agreement with Seattle Parks and Recreation (SPR), DSA is managing activation of Westlake and Occidental Square Parks and has been tracking daily attendance at these parks by having staff count park users at regular intervals each day. DSA is now requesting the City and SPR allow for the installation and powering of sensor devices at select City-owned light poles. The purpose is to significantly improve knowledge of when, and to what degree, downtown parks are used. This will provide a much-enhanced tool to measure the effects of activation and public space management efforts in Westlake and Occidental Parks and at other parks in Downtown, such as Bell Street Park and Freeway Park. It will also inform planning efforts for future activation and for capital improvements. DSA will fund, contract, and manage the project.

The project will track how many people frequent the parks twenty-four hours a day, seven days a week, year-round. The project will be implemented by a vendor (MotionLoft) contracted by DSA. As currently proposed, DSA would provide data summaries to the City at regular intervals throughout the year. These summaries could be shared publicly online, if so desired. This aspect of the proposal may be negotiable. Further research will be required.

Use of personal information

The MotionLoft sensors take a video frame, analyze it, and determine if a moving object is a pedestrian, vehicle, or animal. The video frame does not leave the sensor device and is not stored on the sensor device. The technology collects data related to the number of pedestrians, direction of travel, date, time, weather, temperature, precipitation, latitude, longitude, and events. The video frame is immediately deleted after the moving object is identified. No personally identifiable information (PII) is transferred or stored, either locally or in the cloud. The pedestrian counts and associated metadata, are stored in a database in Amazon Web Services (AWS) - GovCloud. The pedestrian counts and associated metadata, are encrypted in-transit, and do not touch the public internet at any point. The AT&T network is used for transporting the data.

Data Sharing

Summaries of the pedestrian counts, and associated metadata will be public and may be shared online or distributed to an email distribution list.

Technology

The sensor will be mounted on a City-owned pole. The technology analyzes video frames in real time. The video frames used for the analysis are discarded once the analysis is complete. The analysis determines if the frame contains a pedestrian, vehicle, or animal. The pedestrian counts are then sent to the database in the Amazon Web Services (AWS) - GovCloud. Additional fields captured include: date, time, direction, weather, temperature, precipitation, latitude, longitude, and events. All Amazon Web Services (AWS) - GovCloud servers are U.S. based. No data is stored locally on the sensor device. Customers have access to a dashboard which is accessed via a username and password. The data can also be accessed via an application program interface (API) and requires a private key. The data is encrypted during transit, though not at rest. The data at rest does not contain PII. Only pedestrian counts and associated metadata are stored. AES256-bit encryption is used for the data in transit. The OS on the sensor is Linux. The

application and Linux OS can be updated remotely. The MotionLoft team can access the sensor via Secure Shell (SSH). Audit logs capture all sensor activity**,** access to the sensor, and Amazon Web Services (AWS) – GovCloud database access. There is no USB port on the sensor device. The only method that could be used to communicate with the sensor is via a serial port. The sensor does not have any Wi-Fi or Bluetooth capability. The underlying software that is used is ComputerVision. Unusual activity on the sensor is monitored and alerts are generated. The sensors do not have any audio capability. The sensor device has a quad-core processor, so it does not have the processing power to stream data. No images are cached locally on the sensor.

NOTIFICATION

1. ***How does the project/program provide notice about the information that is being collected?*** *Our Privacy Principles and Statement require that we provide notice to the public when we collect personal information, whenever possible.*
   - *Describe how notice will be provided to the individuals whose information is collected by this project/program and how it is adequate.*
   - *If notice is not provided, explain why not. (For certain law enforcement or other project/programs, notice may not be appropriate.)*
   - *Discuss how the notice provided corresponds to the purpose of the project/program and the stated uses of the information collected.*

   A public information campaign will be conducted by both DSA and SPR employing press releases, social media, and on-site signage prior to and during installation of the sensors. Information flyers about the sensors will be available at the park kiosks. Park staff and DSA staff will be informed on the MotionLoft sensors so that they will be able to respond to park-user inquiries. Kiosks are open, and staff are on site from 8AM to 8PM.

2. ***What opportunities are available for individuals to consent to the use of their information, decline to provide information, or opt out of the project/program?*** *Describe how an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. Note: An example of a reason to not provide an opt-out would be that the data is encrypted and therefore unlikely available to identify an individual in the event of a data breach.*

   Individuals will be able to opt-out by avoiding entry to the parks where sensors are installed.

COLLECTION

3. ***Identify the information, including personal information, that the project/program collects, uses, disseminates, or maintains.*** *Explain how the data collection ties with the purpose of the underlying mission of the department.*

Keeping the City downtown parks safe, welcoming, and active, is a priority for the Seattle Parks and Recreation Department. Accurate pedestrian counts will assist in that work.

The sensors will take a video frame, analyze it, and will determine if the moving object is a pedestrian, vehicle, or animal, and will subsequently transfer and store only the pedestrian counts, and associated metadata. The transferred and stored data includes: direction of travel, date, time, count, weather, temperature, precipitation, latitude, longitude, and events. The video frame is deleted immediately after it is analyzed. The video frame does not leave the sensor device and is not stored or cached on the sensor device. No PII is collected, transferred, or stored. Only the pedestrian counts, and associated metadata are transferred to the Amazon Web Services (AWS) - GovCloud cloud.

The accumulated count data will be used to significantly improve knowledge of when -- and to what degree -- downtown parks are used, providing an enhanced tool to: 1) measure the effects of existing activation and public space-management efforts in Westlake and Occidental Parks and at other parks in Downtown, and 2) inform planning efforts for future activation and management, and for capital improvements.

4. ***Is information being collected from sources other than an individual, including other IT systems, systems of records, commercial data aggregators, publicly available data and/or other departments?*** *State the source(s) and explain why information from sources other than the individual is required.*

   There are no additional sources used for the collection or reporting on this data. Pedestrian counts and associated metadata are captured, transferred, and stored for summarization of park use and for reporting. The video frame is deleted after it is analyzed and is not stored or cached locally or in the cloud.

USE

5. ***Describe how and why the project/program uses the information that is collected****. List each use (internal and external to the department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used.*

   Pedestrian count summaries will be used by both DSA and SPR to better understand how the parks are used and how the public responds to various efforts to activate the spaces. The counts will also be used to inform planning and decision-making regarding improvements to activation efforts and to the design of the spaces.

6. ***Does the project/program use technology to:***
   a. ***Conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly or***
   b. ***Create new information such as a score, analysis, or report?***

   If so, state how the City of Seattle plans to use such results. Some project/programs perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Explain what will be done with the newly derived information. Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data?

No information will be collected, transferred, or stored about an individual. All information will be aggregated and summarized. The video frame is deleted after it is analyzed. It is neither stored on the sensor device, nor in the Amazon Web Services (AWS) - GovCloud cloud.

7. ***How does the project/program ensure appropriate use of the information that is collected?*** *Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

   The pedestrian counts, and associated metadata are encrypted when sent to Amazon Web Services (AWS) – GovCloud. All data is collected and stored in the United States. A private key is required to access the API. Generated audit logs capture sensor access and activity, dashboard access, and database access. No PII is collected or stored. Only the pedestrian counts, and associated metadata are transported and stored in the AWS-GovCloud. The video frame is deleted once analyzed. No video frame data is stored or cached locally. No data transits occur over the internet; all transports are over the AT&T network. The sensor does not have Bluetooth or Wi-Fi capabilities. Monitoring software will be in place to alert on unusual activity. There are no microphones on the sensor. A username and password are required to access the MotionLoft dashboard.

RETENTION

8. ***Does the project/program follow the City records retention standard for the information it collects?*** *Departments are responsible for ensuring information collected is only retained for the period required by law. City departments are further responsible for reviewing and auditing their compliance with this process. For more information, please see the internal retention schedule, here, and records retention ordinance, here.*

   In addition, please provide answers to the following questions:
   - *How does it dispose of the information stored at the appropriate interval?*
   - *What is your audit process for ensuring the timely and appropriate disposal of information?*

   The project will work with City Records and follow the appropriate retention schedule. The records retention schedule will be included in the MotionLoft contract.

SHARING

9. ***Are there other departments or agencies with assigned roles and responsibilities regarding the information that is collected?*** *Identify and list the name(s) of any departments or agencies with which the information is shared and how ownership and management of the data will be handled.*

   Data summaries generated from pedestrian counts and associated metadata will be public and may be shared online or distributed to a list.

10. ***Does the project/program place limitations on data sharing?***
    Describe any limitations that may be placed on external agencies further sharing the information provided by the City of Seattle. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment.

The pedestrian counts, and associated metadata stored in the database in the Amazon Web Services (AWS) - GovCloud is not PII. The video frame is deleted after analysis and is not stored locally. The data will be summarized for reporting. No limitations will be placed on sharing the summarized data.

11. ***What procedures are in place to determine which users may access the information and how does the project/program determine who has access?*** *Describe the process and authorization by which an individual receives access to the information held by the project/program, both electronic and paper based records. Identify users from other departments who may have access to the project/program information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project/program information. Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication).*

    MotionLoft requires a username and password to access their dashboard. If the API is used a private key is required. MotionLoft personnel have administrative usernames and passwords. These credentials are used to Secure Shell (SSH) into the sensor device for maintenance and troubleshooting the sensor device. device.

12. ***How does the project/program review and approve information sharing agreements, MOUs, 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.*

    Only pedestrian counts and associated metadata are transported and stored. The video frame is deleted after analysis, no PII is transferred or stored, and the video frame is not stored locally on the sensor device. SPR's relationship will be with the Downtown Seattle Association, not MotionLoft. We have no agreement to access MotionLoft's system. Our agreement will require regular reporting of their data. MotionLoft may also provide limited access as a method of providing reporting information.

LEGAL OBLIGATIONS AND COMPLIANCE

13. ***Are there any specific legal authorities and/or agreements that permit and define the collection of information by the project/program in question?***
    - *List all statutory and regulatory authority that pertains to or governs the information collected by the project/program, including the authority to collect the information listed in question.*
    - *If you are relying on another department and/or agency to manage the legal or compliance authority of the information that is collected, please list those departments and authorities.*

    The City of Seattle's Privacy Policy and Program, the Open Data Policy, the updated Surveillance Ordinance, and any other applicable SPR ordinances will be integrated into the agreement to be established with DSA. After analysis of the regulations and ordinances, the requirements will mandate what the agreement should contain.

14. ***How is data accuracy ensured?*** *Explain how the project/program checks the accuracy of the information. If a commercial data aggregator is involved describe the levels of accuracy required by*

the contract. If the project/program does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project/program.

The MotionLoft sensors transport and store only the sensor counts and associated metadata. The sensors are considered to be reliable and have been implemented and used successfully in San Francisco, New York, New Orleans, Long Beach, and Minneapolis.

15. ***What are the procedures that allow individuals to access their information?***
Describe any procedures or regulations the department has in place that allow access to information collected by the system or project/program and/or to an accounting of disclosures of that information.

The data summaries generated from the pedestrian counts and associated metadata will be public and may be shared online or distributed to a list.

16. ***What procedures, if any, are in place to allow an individual to correct inaccurate or erroneous information?*** *Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If none exist, please state why.*

Once the project has been approved and the MotionLoft technology has been chosen, a system security plan will be completed. The system security plan and contract will contain a dependency that a MotionLoft sensor will be made available in-house to Seattle IT for security scanning and review purposes. There will be a requirement in the contract stipulating all security patches will be applied to the Linux OS and the sensor application.

17. ***Is the system compliant with all appropriate City of Seattle and other appropriate regulations and requirements?*** *Please provide details about reviews and other means of ensuring systems and project/program compliance.*

This PIA has been completed prior to a full review of how the project relates to the City of Seattle's Privacy Policy, Open Data Policy, and the updated Surveillance Ordinance. Such a review will be required before the project moves to implementation.

18. ***Has a system security plan been completed for the information system(s) supporting the project/program?*** *Please provide details about how the information and system are secured against unauthorized access.*

Once the project has been approved and the MotionLoft technology has been chosen, a system security plan will be completed. The system security plan and contract will contain a dependency that a MotionLoft sensor will be made available in-house to Seattle IT for security scanning and review purposes. There will be a requirement in the contract stipulating all security patches will be applied to the Linux OS and the sensor application

19. ***How is the project/program mitigating privacy risk? G****iven the specific data elements collected, discuss 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.*

The video frame of the pedestrian is not stored, cached, or transported. If a sensor device were stolen or hacked, there is no data that could be retrieved; the MotionLoft sensor technology only transports and stores pedestrian counts and associated metadata. The video frame is deleted after it is analyzed. Any risk is more accurately described as a concern, and lies only in the public's *perception* of the sensor rather than the actual data collected. The project will include a campaign targeting public awareness of the capability of the MotionLoft pedestrian counting sensors.

MONITORING AND ENFORCEMENT

20. *Describe how the project/program maintains a record of any disclosures outside of the department.* *A project/program may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project/program keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the project/program must be able to recreate the information noted above to demonstrate compliance. If the project/program does not, explain why not.*

The MotionLoft sensor technology transports and stores only pedestrian counts and associated metadata. No PII is collected, transported, or stored. The video frame is deleted after analysis and is not cached locally on the sensor device. The pedestrian counts, and associated metadata will be summarized and used for reporting. The pedestrian counts, and associated metadata will be summarized and used for reporting.

21. *Have access controls been implemented and are audit logs are regularly reviewed to ensure appropriate sharing outside of the department?* *Is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies? Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

There is no Memorandum of Understanding, contract, or agreement in place with outside agencies; the MotionLoft sensor technology transports and stores only pedestrian counts and associated metadata. No PII is collected, transported or stored. The video frame is deleted after analysis, and is not cached locally on the sensor device. The pedestrian counts, and associated metadata will be summarized and used for reporting. MotionLoft requires a username and password to access their dashboard. If the API is used a private key is required. Audit logs capture all sensor activity**,** access to the sensor, and Amazon Web Services (AWS) - GovCloud database access.

22. *How does the project/program ensure that the information is used in accordance with stated practices of the project/program?* *What auditing measures are in place to safeguard the information and policies that pertain to them? Explain whether the project/program conducts self-audits, third party audits or reviews.?*

The MotionLoft sensor technology transports and stores only pedestrian counts and associated metadata. No PII is collected, transported or stored. The video frame is deleted after analysis and is not cached locally on the sensor device. The use of this sensor is in accordance with the stated practices of the project. The pedestrian counts, and associated metadata will be summarized and used for reporting.

23. ***Describe what privacy training is provided to users either generally or specifically relevant to the project/program.*** *City of Seattle offers privacy and security training. Each project/program may offer training specific to the project/program, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to personal information are trained to handle it appropriately. Explain what controls are in place to ensure that users of the system have completed training relevant to the project/program.*

    There is no privacy training specific to the project; the MotionLoft sensor technology transports and stores pedestrian counts and associated metadata. No PII is collected, transported, or stored. The video frame is deleted after analysis, and is not cached locally on the sensor device. All SPR employees are required to complete the annual Privacy and Security online training course.

24. ***Is there any aspect of the project/program 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.*

    One aspect of the project may cause concern among uninformed members of the public who may mistakenly assume that the sensor devices are serving as surveillance cameras. It will be important to retain on-site information regarding the sensors and to be prepared to provide complete information to any who request information or express concern.