Privacy Impact Assessment

Mobile Pay Parking

PIA-2014-005

Why do I need to do a PIA?
Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA.

Part 1 – General

Name of Department/Branch:	Engineering, Parking Services		
PIA Drafters:	Rob Gordon and Ismo Husu		
Email:	rgordon@victoria.ca	Phone:	250.361.0347
Program Manager:	Ismo Husu		
Email:	ihusu@victoria.ca	Phone:	250.361.0330

1. Description of the Initiative

In 2007 the City created a Parking Strategy document that identified the use of technology to improve customer service. One of the outcomes was the replacement of parking meters with pay parking stations. Another strategy is offering different payment methods. The City currently offers the following pay parking methods:

- Credit card
- Cash
- City parking card.

The City is now in the process of developing a new service whereby people can pay for parking using their mobile devices (e.g. cell phones). The Mobile Parking Payment System Business Requirements Document ("BRD") identified these objectives:

- Improved customer service by adding an additional pay parking method.
- Reduce credit card charges, paper costs and coin processing fees the City incurs.
- To help meet the City's 2015 targets regarding payment methods (e.g. 35% by phone, 40% by coin, and 25% by credit card).
- To save $20,000.00 a year, beginning in 2017, in coin processing costs.

The BRD also identified the following benefits:

- People will not need to rely on coins as much and can add parking time without going back to their vehicles.
- People will not get as many parking tickets.
- Public Service Centre staff will spend less time adding parking time to City parking cards.

- Fewer times to empty coin operated parking meters.
- Reduces maintenance costs (e.g. fewer times to change paper in pay parking stations).
- Other Cities have found that customer relationships improve, enforcement complaints are reduced and businesses can offer to extend parking time thus providing them with a new customer service option.
- Aligns with the City's Strategic Plan.
- Reduces paper costs.
- Helps develop the knowledge and expertise to migrate other, paper-based, services to an online environment.

2. Scope of this PIA

The RFP (14-011) for a mobile parking payment system sought a proponent who could deliver a system that could be used with the City's current on-street parking meter systems. Initially, Passport will only be available for on street parking.

The successful proponent had to provide these deliverables:

- Customers could set up an online account with the City.
- Customers could pay for parking for any 4 digit on-street parking space from this account using their cell phone, tablet or computer without incurring any additional costs.
- Customers could choose to either purchase a set amount of time or use a log in/off process.
- Customers would receive receipts online and be able to review their transaction history
- Customers would receive parking expiration reminders.

PassportParking Inc. ("Passport") was the successful proponent. The City is currently working with Passport to implement its system. This PIA reviews Passport' Mobile Parking Payment System for compliance with FIPPA's privacy provisions.

3. Related Privacy Impact Assessments

There is no previous PIA, but Parking Services Division is currently working on a parking fines debt collection PIA.

4. Elements of Information or Data

1. **Registration Personal Information:** 10 digit mobile phone information (identifies you as authorized user of account), first and last name and email address.

2. **Parking payment personal information:** Vehicle licence plate number, PIN (user password) and email address.

3. **Parking personal Information:** The system generates a parking history that includes: civic address where you parked, the date you parked and how long you parked. This information is linked to your name, email address and vehicle licence plate number.

4. **Credit card:** Your name, type of credit card (Visa, M/C, AMEX, Discover card), card number, expiry date, and postal code.

5. **Location Information:** Our application collects in real-time your device's location for the purpose of linking the particulars of your parking payment (e.g. amount, parking location, parking time) to the City of Victoria's pay parking system. The App uses GPS to identify your location. Your mobile device must have GPS turned on in order to use the APP.

6. **Device Information:** If you download our application, we collect your mobile device ID to notify you of how much time paid you have left on your parking stall.

Personal Information ParkVictoria creates:

A Parker ID is created that resides on the mobile device. It is used to identify every user as unique from every other user.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Passport uses Quebec based iWeb to store the personal information

Physical/technical security: Its servers are isolated servers within their server hosting system. The operating system boundaries and firewall boundaries protect our servers from other systems running on iWeb. SSL Support, Bot protection, DDoS protection, firewalls.

Governance: SAS 70 Type II, SAS 70 protocols

> "*A service auditor's examination performed in accordance with SAS No. 70 represents that a service organization has been through an in-depth examination of their control objectives and control activities, which often include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers*."

Security features for system maintenance, patch updates, synchronization: Firewalls, DDoS protection, SAS 70 protocols

Transmission security: SSL (secure socket layer) communication, API keys (Application Programming Interface keys are like a unique identifier to confirm who is requesting the personal information), Session keys (encryption method).

Back-up locations of personal information: Backup servers are automatically stored on iWeb backup services. These storage locations are also in Canada.

Passport staff access to the personal information from outside Canada:

- Brad Powers - administrative access, full access and permission
- Steven Shelby - maintenance access, read access and permissions
- Justin Cruz - maintenance access, read access and permissions

Passport has processes in place to educate and enforce appropriate access and use.

6. Data-linking Initiative*

There is no data-linking of personal information. Commissionaires do not issue tickets any differently. All Passport provides to Parktoria is the space number, parking is paid for and expiry time. Individuals' identities are not known to Commissionaires.

If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The linkage purpose is different from those for which the personal information in each database was originally obtained or compiled;	no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	no

7. Common or Integrated Program or Activity*

If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	yes
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Please provide a diagram and/or table that shows how your initiative will collect, use, and/or disclose personal information (see examples below). Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. It should also outline the flows of personal information wherever it is transmitted or exchanged.

Both a flow diagram and a table must be included if the PIA is related to a common or integrated program or activity or a data-linking initiative.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	Client creates ParkVictoria account	Collection	26(c)
	Client updates account	Collection	26(c)
	Client updates account	Disclosure	33.2(a) and (c)
2.	Client purchases parking time	Use	32(a)
3.	Client parking payment transaction	Use	32(a)
4.	Client parking payment transaction	Disclosure	33.1(1)(i.1)(i) & (ii)

5.	Client adds funds to parking account	Disclosure	33.1(1)(i.1)(i) & (ii)
6.	Client receives notifications	Use	32(a)

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Retention of personal information for longer than required.	Clients can cancel account anytime and their account is deleted four months after their credit card expires. No financial data retained on mobile device.	low	Low
2.	Client financial information	Not stored on mobile devices or retained by City or Passport. Transaction and security are PCI DSS compliant.	low	High
3.	Staff access to ParkVictoria	Only four staff have access and their workstations are password protected. Inappropriate access would lead to disciplinary action and the system has robust audit capabilities.	low	Low
4.	Data back up	Data is backed up to a different location of IWEB with all the same security and protections and all ParkVictoria data is on dedicated servers	low	Low
5.	Personal information on mobile devices	All data is stored on IWEB servers and must be retrieved from them by clients accessing their accounts. Accounts lock after three failed attempts. Access requires a PIN. No financial data stored on devices.	low	medium
6.	Third party access to personal Information	Existing services providers (Aparc, Commissionaires) do not have access to any ParkVictoria personal information		

10. Collection Notice

Personal information will be collected directly from individuals. They will download the Passport parking App from I-Tunes and Google Play to complete the registration. The section 27(2) notification will be placed on mobile devices.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

Please see question 5 in Part 2 for the physical and security measures of the personal information that Passport store and access from a third party Cloud service provider.

Security of mobile devices:

- Only the parker ID (each user's unique identifier) is stored on the cell phone. Everything else is retrieved from servers.

- All communication is encrypted with SSL. All data stored on the device is also encrypted. All connectivity to our servers must begin with a login, which creates a session. All API access is limited to sessions.

- If a device is stolen, 3 failed login attempts locks the account.

- Users are responsible for deleting their accounts within the App. However, credit card information deletes automatically four months after expiration. Personal information in closed accounts is completely deleted from the servers. Only transaction data is saved, but it cannot identify individuals. At this point Passport does not have the capability to close inactive accounts. It has been suggested to Passport that the ability to do so will bring the App much more in compliance with FIPPA.

- Payment transactions are protected at the PCI DSS level 1.

    - **PCI DSS means**: Payment Card Industry Data Security Standards
    - **What it means**: The organization, PCI Security Standards Council, is an industry standard for the security of online financial transactions. Companies sign an agreement with the Council that requires the companies to maintain security standards set by the Council in order to say they are PCI compliant.

- All personal information sharing is limited to OpsMan back office which is controlled by the same security features as our mobile applications (PCI certification & SSL encryption). This means there is no public access to the information and additional security in place to protect it.

12. Please describe the technical security measures related to the initiative (if applicable).

Parking Services staff access the OpsMan (i.e. the back office administration of mobile pay parking system where the personal information resides) from iWeb's Quebec location. No personal information is stored in City servers. The technical security measures are the same as those in Question Five.

13. Does your branch/department rely on any security policies?

Parking Services is not accessible to the public. Workstations are password protected. There is an understanding of the need to protect personal information and staff are now receiving privacy training. However, there are no written security policies.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

The User Management system can lockout all ability to add, delete or edit any user personal information. The ability to make changes to personal information will be restricted to the Manager of Parking Services. The Parking Services Manager would only change people's personal information when the person attempted to make the change, but their application was not allowing them to. In other words, the application encountered a problem (e.g. a bug). The Manager could also reset someone's password if necessary. He has access to change client's name, address and phone number.

The "Least Privilege Principle" has been adopted with ParkVictoria. Although finding the appropriate level of access for all parking services staff is still being refined, only the manager currently has change privileges. Only three other staff have access to ParkVictoria and their access is read only (Jennifer Grey, Karen Asquini and Linda Jones). They manage parking services and already had access to Tempest's Ticketing module. No new staff have been given access to ParkVictoria.

15. Please describe how you track who has access to the personal information.

Opsman currently logs time of access, visited pages and what was viewed and edited.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

Individuals register their own accounts and can update or de-register at any time. Once an individual closes her account it cannot re-activated.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

No. Individuals who cancel their accounts have their personal information deleted. If an individual's credit card expires, her account expires four months later and only transaction data (e.g. date, location, payment amount) is kept which cannot identify an individual.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No

22. Will a personal information bank (PIB) result from this initiative?

No

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Privacy Office Comments

1. If any changes occur with this service that may result in non-compliance with the privacy provisions (e.g. change to the collection, use or disclosure of the personal information), please contact the Information Access and Privacy Analyst for advice prior to implementing the change(s).

2. Follow up with Passport Parking to improve the audit ability so that unauthorized access to ParkVictoria can be identified.

Privacy Impact Assessment
Mobile Pay Parking
PIA-2014-005

Part 7 – Program Area Signatures

Privacy Officer/Privacy Office Representative | Signature | Date: Jan 21, 2015

Program/Department Manager: Ismo Husu, Manager Parking Services | Signature | Date: Jan 21, 2015

Head of Public Body, or designate: Robert Woodland | Signature | Date: 01/28/2015

A final copy of this PIA (with all signatures) must be kept on record.