CITY OF
VANCOUVER

CITY CLERK'S DEPARTMENT
Access to Information & Privacy

File No.: 04-1000-20-2019-150

March 14, 2019

s.22(1)

Dear s.22(1)

Re: **Request for Access to Records under the Freedom of Information and Protection of Privacy Act (the "Act")**

I am responding to your request of March 4, 2019 for:

> **Privacy Impact Assessment for the VanConnect mobile application, from January 1, 2010 to March 4, 2019.**

All responsive records are attached.

Under section 52 of the Act, and within 30 business days of receipt of this letter, you may ask the Information & Privacy Commissioner to review any matter related to the City's response to your FOI request by writing to: Office of the Information & Privacy Commissioner, info@oipc.bc.ca or by phoning 250-387-5629.

If you request a review, please provide the Commissioner's office with: 1) the request number (#04-1000-20-2019-150); 2) a copy of this letter; 3) a copy of your original request; and 4) detailed reasons why you are seeking the review.

Yours truly,

Cobi Falconer, FOI Case Manager, for

Barbara J. Van Fraassen, BA
Director, Access to Information & Privacy

Barbara.vanfraassen@vancouver.ca
453 W. 12th Avenue Vancouver BC V5Y 1V4

*If you have any questions, please email us at foi@vancouver.ca and we will respond to you as soon as possible. Or you can call the FOI Case Manager at 604.871.6584.

Encl.

:ag

Privacy Impact Assessment for Non-Ministry Public Bodies

Open 311 Mobile App

PIA #*04-10040/0000004-2013-01*

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. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?
Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department/Branch:	City of Vancouver – Digital Services		
PIA Drafter:	**Jessie Adcock**		
Email:	Jessie.Adcock@vancouver.ca	Phone:	**604-871-6868**
Program Manager:	**Darcy Wilson**		
Email:	Darcy.Wilson@vancouver.ca	Phone:	**604-871-6657**

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

The city is expanding the current (311) Call Center process by enabling a mobile and internet based channel. The City intends to implement a public facing Open311 Application Programming interface (API) endpoint that provides access to data and services compliant with the Open311 specification. The solution will include a City branded web application and mobile application that allows citizens to submit a service request to the city as an alternative to calling the 311 call centre.

All of these requests will be directed through a hosted solution and then integrated into the city's existing customer relationship management system, (Kana product - Lagan).

The program will be comprised of both a mobile application technology (system) as well as a web-based user interface which allows citizens to report municipal service requests through their mobile devices and the city website. The program will also allow users to review the progress of their requests and allow city staff to notify residents of municipal events or changes.

The basic process of submitting a service request with the mobile application will involve the user selecting a service location from a map, selecting a service request type and choosing options from drop down fields on the nature of the request. They will then have the option to upload a photo of the issue.

There are two methods of submitting a service request:

1. **As an anonymous user there is no obligation to provide any personal information to submit a service request within the request data fields, description, or in the optional photos.**

2. **As a registered user, they must provide an email account and may optionally supply the following personal information; name, telephone number, home and work address as part of the user profile.**

Users will need to expressly consent to the collection and use of personal information that they submit (as well as to its storage and access in the US) and to comply with the terms and conditions of use.

The following is a summary of the solution:

- The solution consists of a mobile App and an I-frame that can be embedded on the city web page for the submission of service requests or the viewing of previously submitted requests
- A user may optionally register for an account providing an email account and password
- As a registered user they may optionally update their profile to include their name, home address , work address and phone number
- A user can submit a service request anonymously from either the app or the web page
- The IP of the phone is not stored, just the IP of the provider.
- A token is used for communication back to the app on the status of the request

- A user may choose to upload a picture of the city asset that needs repair and there is a potential that the photos could contain personal information.
- A user may populate a description field where they could potentially enter personal information beyond what the city has requested
- A user may mark the submission as private so that it does not display to the general public
- The city can configure a particular service request type to never show publically (i.e. private)
- All service requests that are not marked as private will be displayed on a map with the user's alias account name so that the user can follow requests in their area if desired. However, users' names, emails, addresses and phone numbers will not be displayed to the public or to other users under any circumstance.
- The city can turn off the public display of pictures by service type as desired
- **Generally, we expect that comments and photos will be about City infrastructure and services and not personal information.** Additionally, the City will review all photos and comments on a regular basis and will not permit public display of any pictures of people or any comments containing personal information, or any information or content that is sensitive or offensive

Additionally, the solution will provide a way for the City to allow 3rd party developers to access the Open 311 API in a managed environment so that developers can build applications and services that further enhance public access to the City's 311 service. Allowing other mobile applications is part of the city's digital strategy but the granting of a 'key' to do so will be under the city's control and discretion (and will not be included within the scope of this PIA – as each application and service will need to be evaluated independently).

2. Scope of this PIA

The initiative is an expansion of the City's current (311) Call Center process, by which citizens can include multi-media information with citizen engagement and service request details – which was not previously available to the general public; in the form of a web 'I-frame" and a mobile app. The scope of this PIA, therefore, is limited to both the "I-frame" and the "mobile app" of the Open 311 initiative.

3. Related Privacy Impact Assessments

None that are known

4. Elements of Information or Data

The technology proposed requires that a request initiated and submitted by a City of Vancouver citizen via a mobile device or city website will be routed and stored on the US vendor's platform that is operated as a cloud based server in the United States.

This process may result in the capture of the following data types:

- (possible) requestor name, email address, contact phone number (but in each case onlyif the individual choses to include that information)
- geographic location of the request (where Geographic Location is required for the service request)
- mobile device / website metadata (for example, IP address of the provider, device type, browser type of the requestor)
- it will be possible for individuals to submit requests anonymously (without providing name or contact details -In the case of anonymous requests only location and device metadata is captured.
- (possible) photos and submission is also optional for certain request types
  City staff will be able to review all comments and photos and remove them from public display if they contain personal content (such as without limitation a face or address) or any offensive or illegal content.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

Information can be accessed from outside Canada, as it is a "cloud" hosted solution using servers based in the United States and managed by PublicStuff LLC.

6. Data-linking Initiative*

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. 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 initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	no
2. The purpose for the linkage 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
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. 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.	

**** Please note: If your initiative involves a "data-linking initiative" or a "common or integrated program or activity", advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). Contact your public body's privacy office(r) to determine how to proceed with this notification and consultation.***

For future reference, public bodies are required to notify the OIPC of a" data-linking initiative" or a "common or integrated program or activity" in the early stages of developing the initiative, program or activity. Contact your public body's privacy office(r) to determine how to proceed with this notification.

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

Personal Information Description

Potentially Personal Information Collected:

- Email account if the user choses to register for an account

- Name, phone number or address if the user chooses to enter this information
- Personal information if they enter this information in the description/comments field
- Photographs showing the subject of the request that may inadvertently contain personal information.

Data Flow Narrative:

a. USER SUBMISSION: User submits a request including an optional photo attachment identifying the subject of the service request, the token of the device, device type, device operating system and the location of the request (either as captured by the device itself or as indicated by the user). The name, phone number, address and e-mail of the user is optional and may be included at their discretion.

b. OTHER USER INTERACTIONS: If a user wishes to be updated on status changes of certain submissions – at that point the device information for other users may also be stored – in order to update on status change

c. INFORMATION TRANSMISSION: The request is routed from the mobile device (or City website) through the device internet connection to the vendor's server.

d. INFORMATION STORAGE: All elements identified in USER SUBMISSION will be captured and stored on the vendor's server.

e. INFORMATION INTEGRATION TO CITY INFRASTRUCTURE: The vendor's server re-configures the service request for submission to the City's internal (311) CRM system where it integrates into the City's infrastructure via web services structure. Some of the elements identified in USER SUBMISSION may be stored on the City's CRM system and used during normal operations or for reporting purposes.

f. MUNICIPAL ACTION ON REQUEST: City staff assigned to respond to the request may access photos on the vendor's server during the assessment of the request and to help them make decisions on how to respond to the request.

g. DATA AVAILABILITY: Depending on the nature of the service request, all or some of the details will be available to the public via the mobile device and city website:

   a. Service Request Type and status
   b. Location (either Civic Address or Point location on a map display)
   c. Description of request

d. Photos (if they are configured for the request type) - can be removed from public display for non-compliance with the terms and conditions)[1]

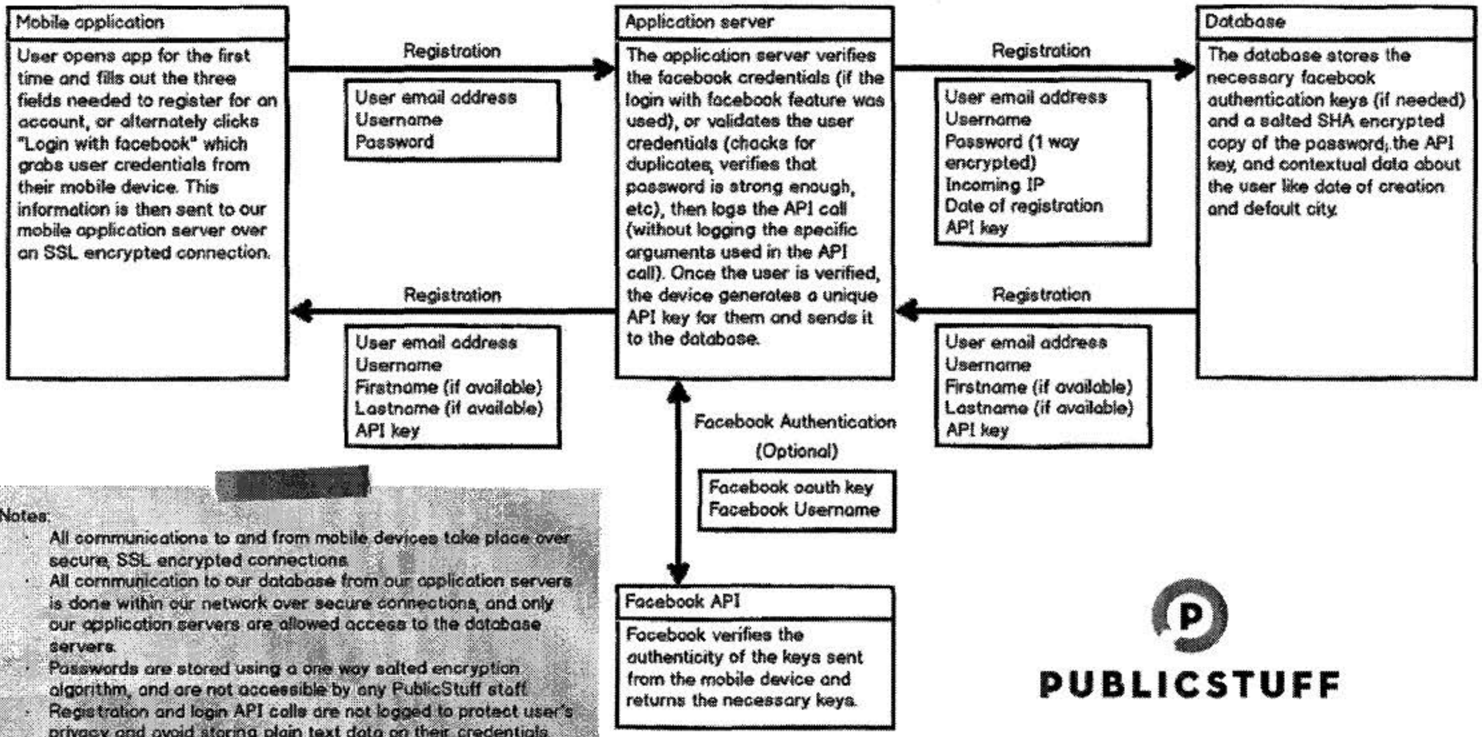
e. The number of "support" actions (similar to social media like) from other citizens

f. Additional comments from other citizens

h. MUNICIPAL UPDATE OF REQUEST: City staff will update request with update status or further details, which will also be transmitted to the vendor server as well as back to the original user (if they chose an option to be updated on status change)

i. DATA AGGREGATION AND REPORTING: City staff may run reports that draw data from the vendor's server on device specific (and potentially other) information. This information may be used to support decisions; measure success/progress and fine tune 311 services over time.

[1] As a component of the business process, photos and videos will be made available for public viewing but will be vetted by City staff to ensure those containing sensitive information are removed from public viewing



Mobile application

User opens app for the first time and fills out the three fields needed to register for an account, or alternately clicks "Login with facebook" which grabs user credentials from their mobile device. This information is then sent to our mobile application server over an SSL encrypted connection.

Application server

The application server verifies the facebook credentials (if the login with facebook feature was used), or validates the user credentials (checks for duplicates, verifies that password is strong enough, etc), then logs the API call (without logging the specific arguments used in the API call). Once the user is verified, the device generates a unique API key for them and sends it to the database.

Database

The database stores the necessary facebook authentication keys (if needed) and a salted SHA encrypted copy of the password, the API key, and contextual data about the user like date of creation and default city.

Facebook API

Facebook verifies the authenticity of the keys sent from the mobile device and returns the necessary keys.

[redacted]

Notes:

- All communications to and from mobile devices take place over secure, SSL encrypted connections.
- All communication to our database from our application servers is done within our network over secure connections, and only our application servers are allowed access to the database servers.
- Passwords are stored using a one way salted encryption algorithm, and are not accessible by any PublicStuff staff.
- Registration and login API calls are not logged to protect user's privacy and avoid storing plain text data on their credentials.
- The IP address logged is not unique to the citizen, but rather a subnet in the data provider's regional network.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	***User Registration*** (mobile app, I-frame) – user email address (if registered user), name, phone number,home address, work address facebook profile name & authkey (for facebook registered user): **User details are collected to associate future service submissions and updates to the citizen.*** ***Prior to registering as a user, a disclosure notification is displayed to the user – upon which the user must accept the disclosure terms and conditions before registration can be completed.*** **User registration is optional; however, updates back to the user on submission status changes will not be available to*	*Collection, Disclosure*	*26(c), 33.2(c)*

	un-registered user submissions.		
2.	User Submission** (mobile app, I-frame) – user email address (if registered user), location, photo and potentially comments : **User submits service or details which they feel are important for City staff to be aware of.** **If a submission occurs as an unregistered user, a disclosure notification is displayed to the user for every submission outlining the details of information storage and privacy impacts.	*Collection, Disclosure*	*26(c), 33.2(c)*
3.	***Other Interactions*** *(mobile app, I-frame) – user email address (if registered user,:* ***Service or details which a citizen has submitted are updated from a city staff – the status changes or questions are communicated back to the citizen in the medium which the submission was made.*** ***There are three variations of Other Interactions:*** ***1) Service Status change for registered user (mobile): the service status change updates the user on their mobile phone when the change occurs.*** ***2) Service Status change for registered user (web): the service status change updates the user at their email address when the change occurs.*** ***3) Service Question for registered user (mobile/web): the service question is sent to email address of registered user, in the event that there is confusion or questions relating to the submission.***	*Use*	*32(a)*
4.	***Information Transmission*** *user email address (if registered user), location, photo, submission details:* ***Submission details are transferred from the citizen via vendor (secure internet connexion) to City Staff (service provider) via City hosted Lagan application.***	*Use*	*32(a)*
5.	***Data Aggregation and Reporting*** *all data associated with the submission (including method of submission, seasonality, location trends, types of submission):* ***City staff may run reports that aggregate data from the vendor's***	*Use*	*32(a)*

	server on various aspects of the submission and methods – which will be used to analyze the service provided and identify opportunities.		

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Employees could access personal information and use or disclose it for personal purposes*	*Employment Policies; contractual terms with vendor; security access rights within the application for information display.* *The level of personal information is limited to the following:* *Email* *Username* *First name (optional)* *Last name (optional)* *Phone number (optional)* *Home address (optional)* *Work address (optional)* *Personal information in the comments or description (optional)* *Personal data in the photo* *Facebook auth key (optional)* *Facebook Username (optional)* *The type of information is limited to only the data that is required for the application to ensure non-repudiation – no extra user metadata is collected.*	*Low*	*Low-Medium*

2.	*Request may not actually be from client (i.e. their email address may be compromised)*	*User registration security procedures; types of submissions available are limited to non-sensitive requests (for example: street light, pothole repair, sidewalk crack)*	*Low*	*Low*
3.	*Client's personal information is compromised when transferred to/from the service provider*	*All communications to and from the service provider take place over secure, SSL encrypted connections.*	*Low*	*Low*
4.	*Inherent risks in sending submission details (including service requests from city staff) via mobile or web interface*	*Notification to inform clients of risk and ask if they would like to submit the information via a different medium they should call 311 to submit the details directly to a call center representative.*	*Low*	*Low*

10. Collection Notice

A full disclosure and consent form with an option to accept or reject will be presented to the users in the following situations:

- The first time the app is opened on the mobile device OR when a web user choses to register for an account
- The user who chooses to submit requests anonymously on the web page will give consent before submitting the request.

The scenarios above will cover all use cases; a user will not be able to submit a request using the Open 311 web or mobile app channel without giving consent. If the user declines, then they will not be able to submit the request and will be required to call 311.

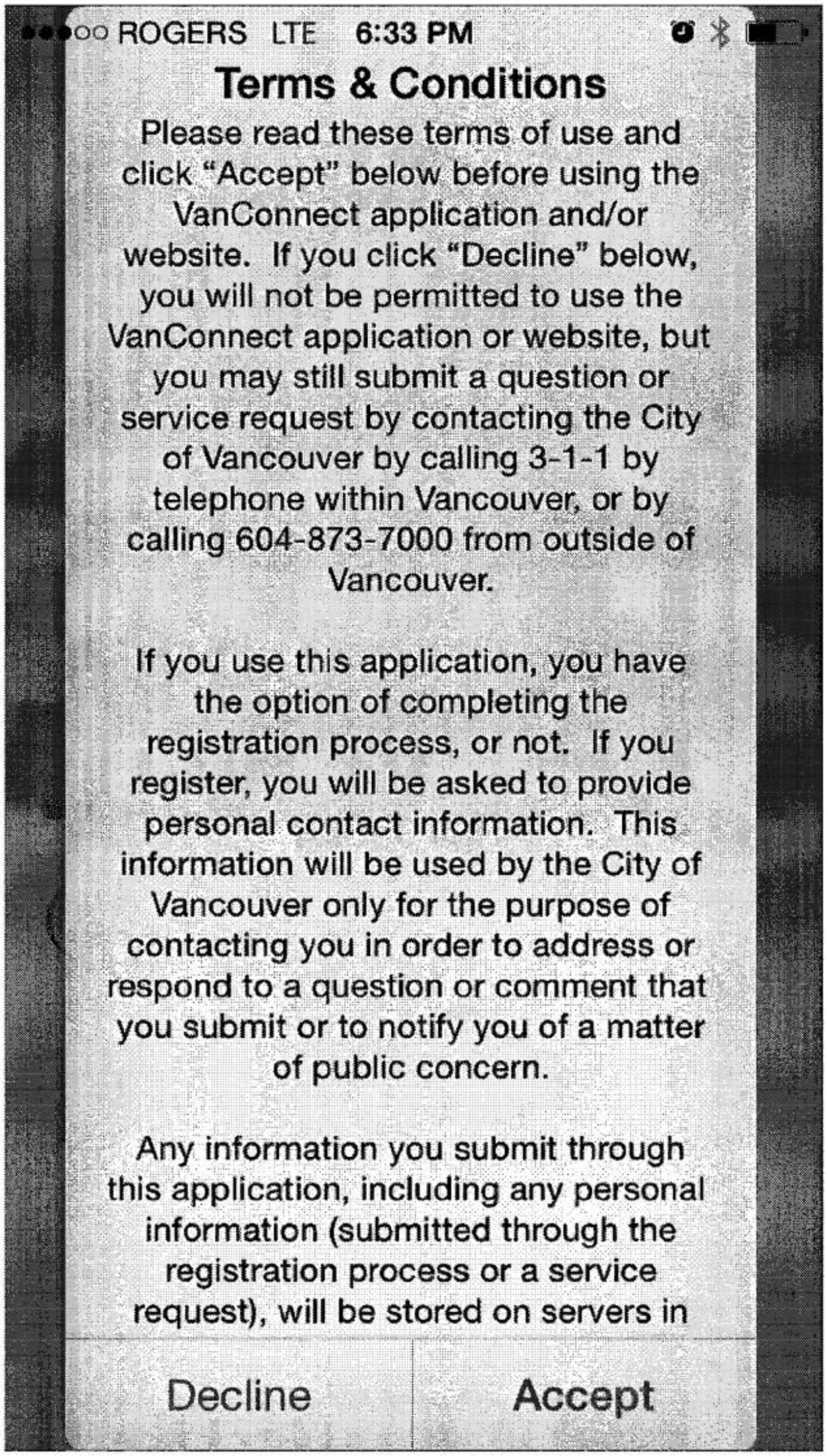
The disclosure statement is as follows:

If you register to use the VanConnect application and/or website or if you use the VanConnect application and/or website to submit information to the City of Vancouver, all of the information that you provide as part of the registration process or otherwise submit at any time, including any personal information, will be stored on servers in the United States and may in the future be stored on other servers elsewhere outside Canada. By clicking 'Accept' below, you agree that you have the legal capacity to consent, and that you do consent, effective as of the present date, to any personal information that you submit being stored in the United States or elsewhere by PublicStuff Inc., which operates the VanConnect application and website on behalf of the City of Vancouver, and to such information being accessed by PublicStuff Inc. or by employees or agents of PublicStuff Inc., for the purpose of allowing PublicStuff Inc. to maintain and operate the VanConnect application and website and transmit your submitted information to the City of Vancouver. Whether or not you click 'Accept' below, you are not obligated to provide any personal information in order to use the VanConnect application or website. If you provide contact information, including contact information that constitutes personal information, it will be used by the City of Vancouver only for the purpose of contacting you in order to address or respond to a question or comment that you submit or to notify you of a matter of public concern. By clicking 'Accept' below, you agree that the personal information that you provide to us may be collected and used for the aforesaid purposes. If you click 'Decline' below, you may, instead of using the VanConnect application or website, contact the City of Vancouver by calling 3-1-1 by telephone within Vancouver, or by calling 604-873-7000 from outside of Vancouver.

Personal information is collected by the City of Vancouver under the authority of the Freedom of Information and Protection of Privacy Act. Questions may be directed to the Director, Access to Information at 453 West 12th Avenue, Vancouver, British Columbia V5Y 1V4 or via telephone at 604-873-7999

Decline *Accept*

Screenshot of Disclosure Statement from the Mobile App:

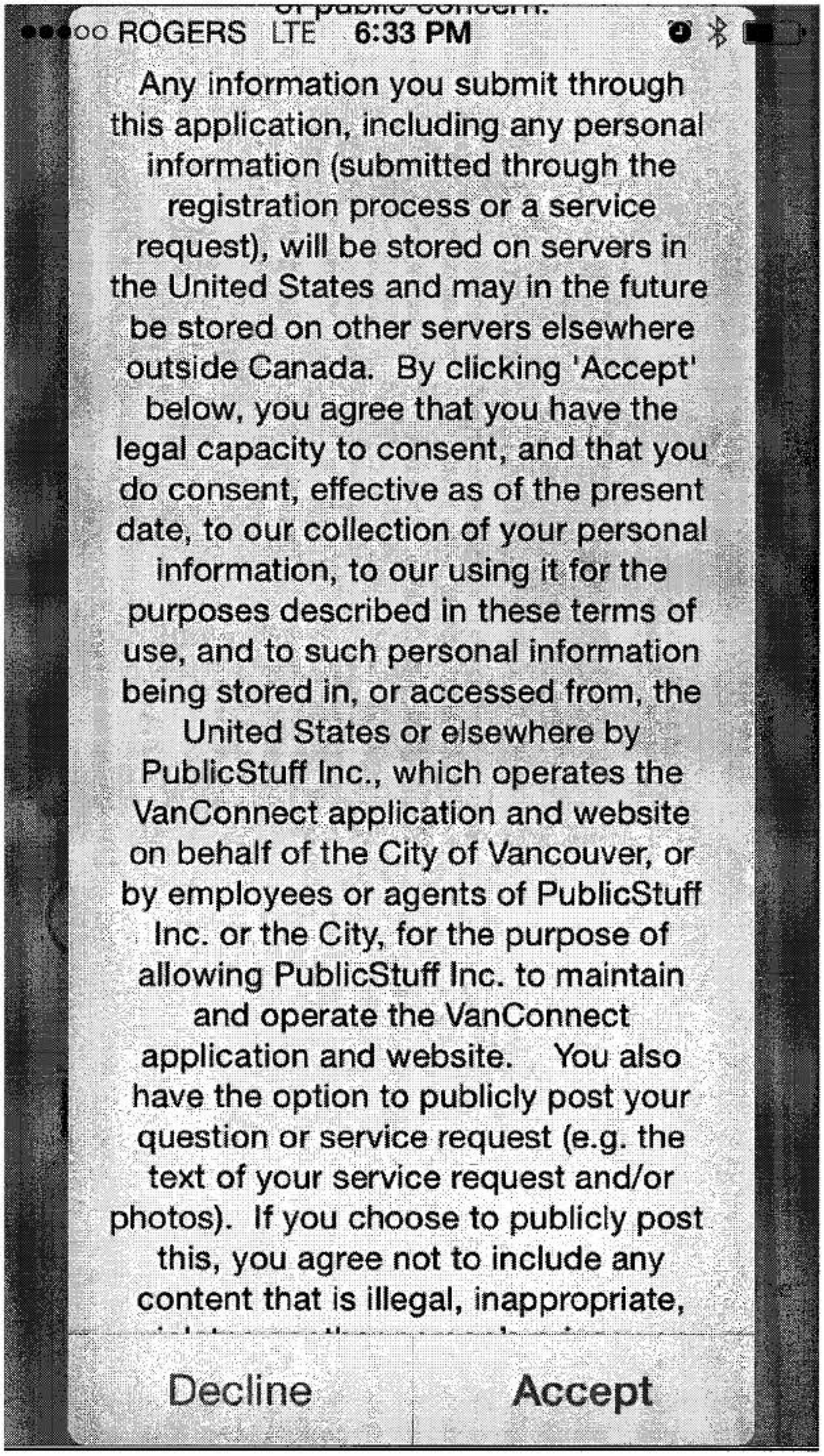


Terms & Conditions

Please read these terms of use and click "Accept" below before using the VanConnect application and/or website. If you click "Decline" below, you will not be permitted to use the VanConnect application or website, but you may still submit a question or service request by contacting the City of Vancouver by calling 3-1-1 by telephone within Vancouver, or by calling 604-873-7000 from outside of Vancouver.

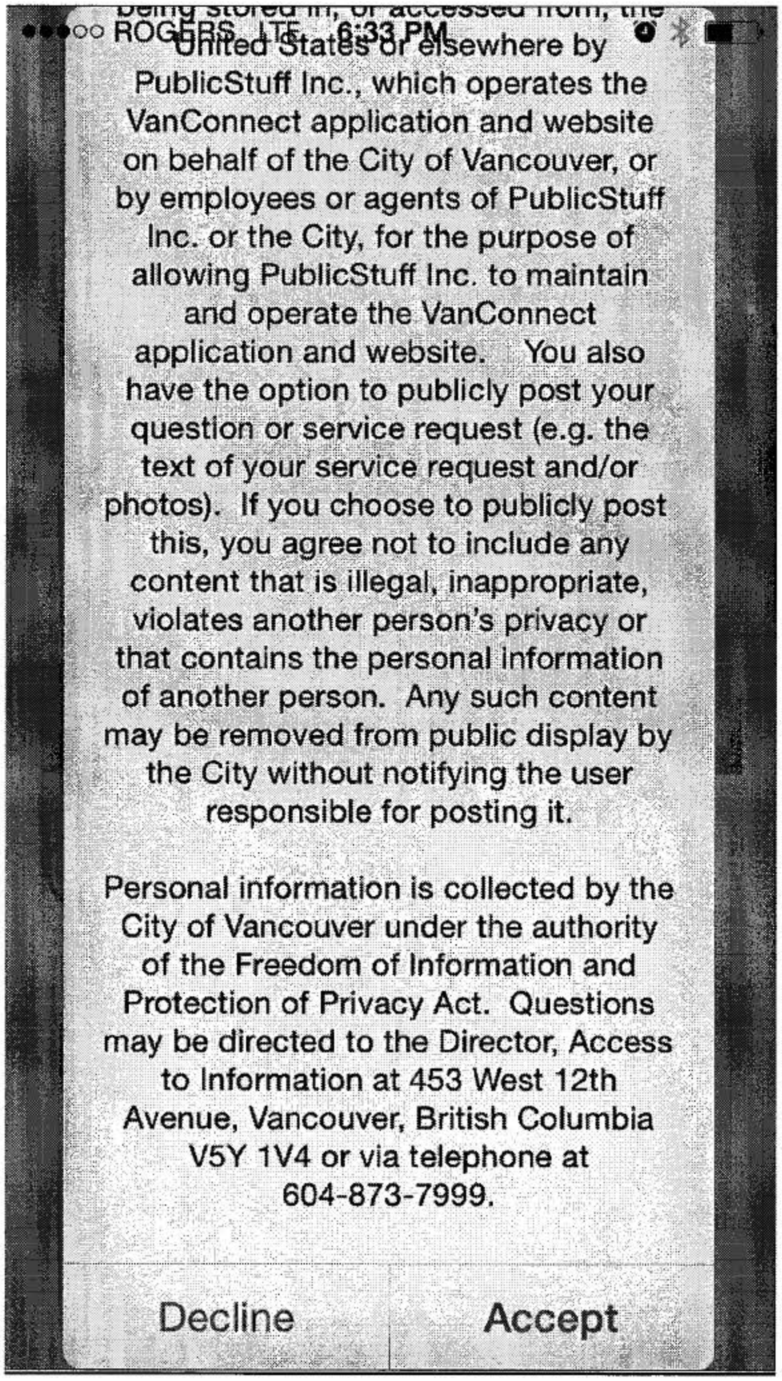
If you use this application, you have the option of completing the registration process, or not. If you register, you will be asked to provide personal contact information. This information will be used by the City of Vancouver only for the purpose of contacting you in order to address or respond to a question or comment that you submit or to notify you of a matter of public concern.

Any information you submit through this application, including any personal information (submitted through the registration process or a service request), will be stored on servers in



of public concern.

Any information you submit through this application, including any personal information (submitted through the registration process or a service request), will be stored on servers in the United States and may in the future be stored on other servers elsewhere outside Canada. By clicking 'Accept' below, you agree that you have the legal capacity to consent, and that you do consent, effective as of the present date, to our collection of your personal information, to our using it for the purposes described in these terms of use, and to such personal information being stored in, or accessed from, the United States or elsewhere by PublicStuff Inc., which operates the VanConnect application and website on behalf of the City of Vancouver, or by employees or agents of PublicStuff Inc. or the City, for the purpose of allowing PublicStuff Inc. to maintain and operate the VanConnect application and website. You also have the option to publicly post your question or service request (e.g. the text of your service request and/or photos). If you choose to publicly post this, you agree not to include any content that is illegal, inappropriate,



being stored in, or accessed from, the

●●●○○ ROGERS LTE 6:33 PM

United States or elsewhere by PublicStuff Inc., which operates the VanConnect application and website on behalf of the City of Vancouver, or by employees or agents of PublicStuff Inc. or the City, for the purpose of allowing PublicStuff Inc. to maintain and operate the VanConnect application and website. You also have the option to publicly post your question or service request (e.g. the text of your service request and/or photos). If you choose to publicly post this, you agree not to include any content that is illegal, inappropriate, violates another person's privacy or that contains the personal information of another person. Any such content may be removed from public display by the City without notifying the user responsible for posting it.

Personal information is collected by the City of Vancouver under the authority of the Freedom of Information and Protection of Privacy Act. Questions may be directed to the Director, Access to Information at 453 West 12th Avenue, Vancouver, British Columbia V5Y 1V4 or via telephone at 604-873-7999.

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

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

PublicStuff laptops hard drives are encrypted and password protected, and stored in a padlocked locker when not in use. The building is locked with a keycard, and managed by a doorman during extended business hours. All our data is stored in Rackspace hosted database servers, which can only be accessed directly by the CTO and system administrator. Code is stored in a set of private repositories on Github.

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

PublicStuff database and application servers are both positioned behind a firewall on Rackspace servers. All transmissions from our mobile applications are encrypted during transmission and validated using a 3rd party verified SSL certificate.

COV technical security measures receiving the information from Public Stuff include the initial server receiving the information is contained within a DMZ(with firewall protection that is continually being monitored and updated) – which allows for COV to ensure no malicious data or code enters the COV data network. Communication between the COV server and PublicStuff server occurs using HTTPS protocol and secure SSL ports. All requests to and from COV servers are logged for audit purposes.

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

Yes – as dictated by City of Vancouver IT Security policy.

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 vendor's policy (PublicStuff) is to only discuss specific security details with members of the security team, but they do limit access and log any changes to the system and database by engineers, users, and administrators.

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

The vendor's (PublicStuff) has audit trails and logs all connections to servers. The vendor's (PublicStuff) only allows need based access to specific files or systems as approved by management.

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?

Registered Users will have the ability to update their registration details (to either add or remove information from their registered profile). Un-registered users or anonymous users of the system will not have any personal details stored within the cloud hosted database.

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?

N/A

Part 5 – Further Information

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

No

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	□

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

No

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	□

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

No

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

Part 7 – Program Area Signatures

Darcy Wilson		March 10 / 2015
Program/Department Manager	Signature	Date
Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date
Jesse Adcock		March 10/2015
Chief Digital Officer (Designate for Head of Public Body)	Signature	Date

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

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

Barbara J. Van Fraassen Director, Access to Information		MARCH 10, 2015
Privacy Officer/Privacy Office Representative	Signature	Date