

PRIVACY IMPACT ASSESSMENT – MTICS14027

I BASIC INFORMATION - New or Existing Program, System or Legislation

1. Ministry/Public Body and Program Area.

Ministry	Ministry of Technology, Innovation and Citizens' Services
Division	Office of the Chief Information Officer
Branch/Section	Privacy and Legislation Branch
Initiative Title	Use of Online Applications and Software not involving personal information

2. Contact Position and/or Name, Telephone Number and E-Mail Address.

(This should be the name of the individual most qualified to respond to questions regarding the PIA).

Name, Title	Matt Reed
Branch/Section	Privacy and Legislation Branch
Phone Number	250-514-8870
E-Mail	Matt.Reed@gov.bc.ca

3. Description of the Program/System/Legislation (Initiative) being assessed.

(Please note here if the initiative does **not** collect, use or disclose personal information). If this is a change to an existing legislation, system or program, describe the current system or program and the proposed changes.

Government is moving towards more prevalent use of mobile applications ("applications") and downloadable software ("software"). Applications are downloadable programs that provide a variety of functions or services. Apps are downloaded to a device, normally through an app store or directly from the app vendors' websites. Once on a device, the app can be used in the manner set out by its creator. Similarly, software is downloaded to a device from vendor websites or aggregated download sites (e.g. download.com).

"Categories" in which applications and software can be downloaded include but are not limited to: books, business, catalogues, education, entertainment, finance, news, productivity, and reference. This PIA addresses applications and software in all "categories". This PIA can apply to all categories of applications and software because the evaluated criteria of this PIA is not the function of the application or software, but whether or not they involve personal information. Some examples of apps include: Clinometer+ (app that measures slope); Google Maps (app that provides maps, directions); Evernote (app that allows note-taking); Prezi (app that allows presentation-creation). Some examples of software include: Fusion (a program for reading forestry analyses), FireFox (an internet browser); IrfanView (a graphics viewer).

After a government employee has their workstation(s) refreshed, and/or is provided with a "smart" device, they will have the administrative abilities to add/download a new application or software onto their device. This means that each employee is responsible for managing the privacy compliance of their device and the personal information on it and accessible by it. Employees downloading applications and software must adhere to the Appropriate Use directive (Chapter 12 of the Core Policy and Procedures Manual).

Once purchase and download have each, respectively, been approved for the application/software through the appropriate channels, an employee must ensure that the privacy provisions set out in this PIA are met. For example, of the applications listed above (Clinometer+, Google Maps, Evernote and Prezi), each can be used in such a way as to **not** involve personal information. However, each can also be used in ways that do. For example, a social worker may tag a client's folio number to their address in Google Maps, or notes on a client's file might be made in Evernote. **These are example of uses that would not be covered by this PIA.** If an

employee is looking to use an application or software in a way that involves personal information they are required to conduct a separate privacy impact assessment.

This PIA is written to address the download and use of any and all applications and software used by government employees **that do not collect, use, disclose, store or access personal information**. A self-assessment tool has also been developed to help employees evaluate whether or not an application or software (or an employee's use of it) fall within the criteria set out in this PIA. If an application or software (or an employee's use of it) does not fall within the criteria set out in this PIA, the employee will have to conduct a new PIA. Employees falling into this category should contact a privacy analyst at the Legislation, Privacy and Policy Branch, OCIO for help drafting a PIA for these apps.

		*Yes	No
(a)	Does this PIA involve a common or integrated program/activity (as defined in FOIPPA)? and		X
	Is the common or integrated program/activity confirmed by the written requirements set out in the regulation?		X
(b)	Does this PIA involve a data-linking initiative (as defined in FOIPPA)?		X

4. Purpose/Objectives of the initiative (if statutory, provide citation).

The purpose of this PIA is to provide the privacy analysis for all those apps downloaded onto government devices and used by government employees in a way that does not collect, use, disclose, store or access personal information.

The apps that employees download serve a variety of purposes that cannot be summarized here. For the purposes of this PIA, an app can be used for any purpose as long as that purpose does not result in the unauthorized collection, use, disclosure, storages or access of personal information.

5. What are the potential impacts of this proposal? (Include privacy impacts in this description).

There are a number of potential impacts to this proposal. Given the number of apps available for download by government employees, an individual assessment of each one is unfeasible. This PIA addresses the parameters within which all apps must meet. In this way, privacy compliance can be achieved in a time and resource effective way.

As this PIA represents the required PIA for all applications and software that do not involve personal information, there is a risk that employees will presume its coverage for applications and software that may involve personal information. In order to mitigate this risk, we have provided the required information within this PIA to a wide audience within government.

As a part of the Appropriate Use information sessions (which were advertised and open to all of government), this information has been communicated to many employees. Further, guidance documents (e.g. Appendix B) and this PIA will be posted on the PLB website. This PIA will also be accompanied by a self-assessment tool so that employees can quickly and easily make an accurate assessment as to whether or not the application or software in which they are interested is covered by this PIA, or whether it requires an additional PIA. The corporate PIA and checklist approach has proven very successful for social media PIAs, and so we expect it to prove equally successful in this area.

There is also a risk that an application or software – though it may not involve personal information – represents a security risk to government information. This risk is mitigated by the security awareness information provided at the same Appropriate Use sessions. Employees were provided with guidance on how to make an assessment of potential security risks, how to identify when a more in-depth security assessment is required, and who to go to in order to conduct those more in-depth security assessments.

There is a risk that employees will use apps in ways that do not properly comply with FOIPPA (e.g. use the apps in such a way as to involve personal information). In order to help mitigate this risk, a guidance document (e.g. Appendix B, and the Self-Assessment form) has been developed to help employees become aware of how apps should be used and what things they have to watch for (e.g. employees must ensure that apps do not access their Contacts, and must know how to disable that access when an app “requests” it).

In support of all of the above risks, a guidance document separate from this PIA has been developed. It contains background information on the risks that applications and software represent, a copy of the self-assessment, and other considerations. This guidance document is being distributed through the Appropriate Use sessions, and will be posted online as well. The guidance document is attached as Appendix B.

Finally, in support of mitigating all of the above risks, the contents of this PIA and the expected approach for employees will be communicated to the Ministry Chief Information Officers (MCIOs) and Ministry Information Security Officers (MISOs). MCIOs and MISOs, as ministry contacts for matters relating to privacy and security, have their own means for communicating this information out through the appropriate channels within their ministry.

6. Provide details of any previous PIA or other form of personal information assessment done on this initiative (in whole or in part).

N/A

IF THERE IS NO PERSONAL INFORMATION INVOLVED, GO TO X. SIGNATURES.

****IMPORTANT NOTE:** FOIPPA defines personal information as "recorded information about an identifiable individual other than contact information." Contact information includes the name, title, telephone or facsimile number, email address etc., which enables an individual at a place of business to be contacted.

II DESCRIPTIVE INFORMATION

1. Describe the elements of personal information that will be collected, used and/or disclosed and the nature and sensitivity of the personal information. [See note above about the definition of personal information.]

For example: Name, home address, gender, age/birthdate, SIN, Employee#, race/national, ethnic origin.

Applications and software will collect different information based on their function and purpose. In order to be covered by this PIA, the applications and software cannot collect, use, disclose, store or access personal information.

2. Provide a description (either a narrative or flow chart) of the linkages and flows of personal information collected, used and/or disclosed.

N/A – In order to be covered by this PIA, the application or software cannot collect, use, disclose, store or access personal information.

III PERSONAL INFORMATION COLLECTION

(Section 26 and section 27 of the *Freedom of Information and Protection of Privacy Act* "FOIPPA Act")

****IMPORTANT NOTE:** Recent amendments to FOIPPA have clarified when personal information has *not* been collected by a public body. See section 27.1 or contact Knowledge and Information Services for further details.

	Yes	No	n/a
Is personal information being collected?		X	

IF THERE IS NO PERSONAL INFORMATION BEING COLLECTED, GO TO IV. USE OF PERSONAL INFORMATION

IV USE OF PERSONAL INFORMATION - (Section 32 of FOIPPA)

	Yes	No	n/a
Is personal information being used?		X	

IF THERE IS NO PERSONAL INFORMATION BEING USED, GO TO V. DISCLOSURE OF PERSONAL INFORMATION

V DISCLOSURE OF PERSONAL INFORMATION

(Section 33, section 33.1, section 33.2, section 33.3, section 34, section 35 and section 36 of FOIPPA)

	Yes	No	n/a
Is personal information being disclosed?		X	

VII SECURITY AND STORAGE FOR THE PROTECTION OF INFORMATION

		Yes	No	n/a
1.	Is there reasonable technical security in place to protect against unauthorized access or disclosure? Employees must ensure that their devices comply with Information Security Policy and all other applicable security policies. This includes the requirements to have complex password protection on the device.	X		
2.	Is there reasonable physical security in place to protect against unauthorized access or disclosure? Employees must ensure that the device is managed in compliance with the Information Security Policy and all other applicable security policies. This includes compliance with the Information Incident Management Process that dictates that a lost device must immediately be reported to the OCIO.	X		
3.	Are there branch policies and procedures in place for the security of personal information during routine collection, use and disclosure of the information?			X
If yes, please provide the name of the policy and/or procedures, a contact person and phone number.				
	Policy/procedure:	Information Security Policy; Information Incident Management Process, Core Policy and Procedures Manual		
	Contact person:	OCIO		
	Phone number:	7-7000, option 3 (Breach Reporting Line); 250-356-1851 (Privacy and Access Helpline); CITZCIOSecurity@gov.bc.ca (Security Branch Contact email)		
Additional details as required				
4.	Have user access profiles been assigned on a need-to-know basis? Users that are not the employee with responsibility over the device should not be permitted access to the device.	X		
5.	Do controls and procedures exist for the authority to add, change or delete personal information? Applications and software covered by this PIA must not add, change or delete personal information.			X
6.	Does your system security include an ongoing audit process that can track use of the system (e.g., when and who accessed and updated the system)?			X
Please explain the audit process and indicate how frequently audits are undertaken and under what circumstances				
7.	Does the audit identify inappropriate accesses to the system?			X
Additional details				

If any of the questions above have been answered "no", please contact your Ministry's Security Officer. If you have any questions or require clarification please contact Knowledge and Information Services.

VII SECURITY ARRANGEMENTS FOR THE PROTECTION OF PERSONAL INFORMATION
cont'd

Section 30.1 requires a public body to ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada unless the individual the information is about has consented or the disclosure is otherwise allowable under the Act.

		Yes	No	n/a
	Will the information be stored or accessed only in Canada?			X




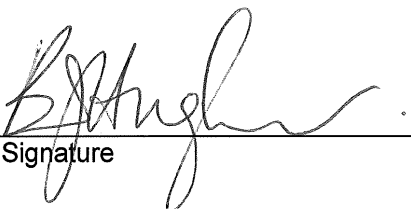
Comments:

If an employee is unsure whether their download/use of an application or software is covered by this PIA, PLB recommends that they complete the self-assessment tool provided as an appendix to this PIA. If, after completing the self-assessment tool, they are still unclear as to whether this PIA covers their download/use of an application or software, they should contact their Ministry Information Security Officer (MISO). MISO contact information can be found here: <https://www.cio.gov.bc.ca/MISO/MISOs.htm>

If this PIA does not cover an employee's download/use of an application or software, they must complete a new General PIA, and submit that PIA through the usual PIA process.

X SIGNATURES

PUBLIC BODY APPROVAL:

<u>Matt Reed</u> Program Manager	<u></u> Signature	<u>JUNE 26, 2014</u> Date
<u>Rob Todd</u> Ministry Contact Responsible for Systems Maintenance and Security	<u></u> Signature	<u>June 26/14</u> Date
<u>Sharon Plater</u> Privacy and Legislation Branch Office of the Chief Information Officer Ministry of Technology, Innovation and Citizens' Services	<u></u> Signature	<u>July 3/14</u> Date
<u>Bette-Jo Hughes</u> Assistant Deputy Minister or Equivalent	<u></u> Signature	<u>3 July 14.</u> Date

GO TO: PERSONAL INFORMATION DIRECTORY (to add PIA and/or ISA summary)

Appendix A

Self-Assessment Tool for Applications and Software

This self-assessment may be completed to determine if a separate PIA is needed (e.g. if you answer “yes” to any question) to address the program area’s needs around the use of an online app or service. For purposes of due diligence, LPP recommends that the branch retain a completed version of this assessment.

Name of application or software: _____
 Name of employee(s)/branch downloading app or software: _____
 Name of Self-Assessment Drafter: _____ Date of assessment: _____

Ask yourself	Yes	No
Privacy If you answer “Yes” to any of the following privacy related questions it is recommended that you contact the OCIO's Legislation, Privacy and Policy Branch at Privacy.helpline@gov.bc.ca or 250-356-1851		
1. Will you be using the application or software to store or send any personal information? <ul style="list-style-type: none"> For example, are you planning to use an application like DropBox to send files with data about individuals, or will you be using Siri to translate client testimony? 		
2. Will the application or software have access to anyone else's personal information, such as their names, personal addresses, and personal phone numbers? <ul style="list-style-type: none"> For example, many applications will want access to your Contacts or Address Book. <p>Note: If the application has an opt-out or decline option on this access, and you will opt out/decline, you may answer “No” to this question.</p>		
3. Does the application have settings that allow it to share information with other applications? <ul style="list-style-type: none"> For example, many applications will want to “connect with your Facebook friends” or link to your contacts in another application/online service. <p>Note: If the application has an opt-out or decline option for these connections, and you will opt out/decline, you may answer “No” to this question.</p>		

Security

If you answer “Yes” to any of the following security related questions it is recommended that you contact your Ministry Information Security Officer (MISO). Contact information for MISOs can be found at the following link: <https://www.cio.gov.bc.ca/MISO/MISOs.htm>

4.	Will the application or software have access to any confidential government information? <ul style="list-style-type: none"> Confidential information includes personal information and other information with confidentiality requirements such as Cabinet confidences, third party business information, confidential advice and recommendations, contract negotiations, and legal advice. Information classified as “sensitive” for the purposes of security classification should also be considered confidential. 		
5.	Does the application require unnecessary or inappropriate access to the network? <ul style="list-style-type: none"> In some cases, an application will require access to the network in order to function properly (e.g., search engines and social media). Other applications (for example games, compasses, and calculators) should not require network access to function. An application may ask for network access so that it can download required updates, but network access can also be used to transfer information off of the device. If the application is asking for access to the network, you should ask yourself whether the application needs that access to perform its intended task. If it doesn't, the application could be putting the network at inappropriate or 		

Ask yourself		Yes	No
	unnecessary risk. If you need assistance in making this determination, you should contact your MISO.		
6.	<p>Are you aware of any concerns about the application's reputation?</p> <ul style="list-style-type: none"> For example, some application stores or providers (e.g., Android) do not currently vet their applications to the same degree as others. While this does not mean that these applications are not safe or suitable (to the contrary, many of these applications are perfectly safe and useful), it may, at least for the near future, warrant some additional consideration. <p>Note: if you have no information on the reputation of the application or its manufacturer, the following sources may help:</p> <ul style="list-style-type: none"> Do an internet search of the application and the manufacturer Check out user reviews of the application Ask your colleagues or Ministry Information Security Officer 		
7.	<p>Is there anything about the application or software, not already addressed above, that concerns you?</p> <ul style="list-style-type: none"> Services available on devices and the threats to devices, privacy and information change all the time and cannot all be addressed in a guidance document such as this. For this reason, if there is anything about the application or software that concerns you or makes you uncomfortable, you should seek advice from your Ministry Information Security Officer. 		

Appendix B – Application and Software Guidance Document

Applications and Software

Privacy and Security Considerations

Applications are a part of our everyday lives; they are used for everything from getting weather reports and directions to tracking our fitness levels and health. Increasingly, applications are becoming part of our professional world as well, helping to increase productivity and facilitate collaboration. At the same time, the Workstation Refresh Project has increased the flexibility that employees have in managing their devices. Employees now have greater choices in the tools that they can use to do their jobs, including which applications and software are used.

While applications and software provide us with additional tools to do our jobs, employees need to be aware of the potential risks to privacy and to the security of government information when using applications and software. Not every application is safe to use for work purposes. As well, some applications and software may impose terms and conditions that are unacceptable to government. For these reasons, the Appropriate Use Policy requires that employees obtain their supervisor's permission before downloading applications or software to their device. This includes downloading applications and software to a workstation as well as to a mobile device, such as a laptop, smartphone or tablet. The requirement to obtain supervisor permission is not meant to be a deterrent to downloading useful applications and software. Rather, it is to ensure that applications and software are downloaded with full knowledge of both their benefits and potential risks.

Ministries may develop specific policies or guidelines to assist supervisors in determining the safety and suitability of applications and software. In the meantime the following guidelines will assist supervisors with this assessment.

Application and Software Checklist

If you answer "Yes" to any of the following questions, there may be privacy or security concerns and it is recommended that you seek further advice or direction.

Ask yourself		Yes	No
Privacy If you answer "Yes" to any of the following privacy related questions it is recommended that you contact the OCIO's Legislation, Privacy and Policy Branch at Privacy.help@bc.ca or 250-356-1851			
1.	Will you be using the application or software to store or send any personal information? <ul style="list-style-type: none"> For example, are you planning to use an application like DropBox to send files with data about individuals, or will you be using Siri to translate client testimony? 		
2.	Will the application or software have access to anyone else's personal information, such as their names, personal addresses, and personal phone numbers? <ul style="list-style-type: none"> For example, many applications will want access to your Contacts or Address Book. <p>Note: If the application has an opt-out or decline option on this access, and you will opt out/decline, you may answer "No" to this question.</p>		
3.	Does the application have settings that allow it to share information with other applications? <ul style="list-style-type: none"> For example, many applications will want to "connect with your Facebook friends" or link to your contacts in another application/online service. <p>Note: If the application has an opt-out or decline option for these connections, and you will opt out/decline, you may answer "No" to this question.</p>		

Security

If you answer "Yes" to any of the following security related questions it is recommended that you contact your Ministry Information Security Officer (MISO). Contact information for MISOs can be found at the following link: <https://www.cio.gov.bc.ca/MISO/MISOs.htm>

4.	Will the application or software have access to any confidential government information? <ul style="list-style-type: none"> Confidential information includes personal information and other information with confidentiality requirements such as Cabinet confidences, third party business information, confidential advice and recommendations, contract negotiations, and legal advice. Information classified as "sensitive" for the purposes of security classification should also be considered confidential. 		
5.	Does the application require unnecessary or inappropriate access to the network? <ul style="list-style-type: none"> In some cases, an application will require access to the network in order to function properly (e.g., search engines and social media). Other applications (for example games, compasses, and calculators) should not require network access to function. An application may ask for network access so that it can download required updates, but network access can also be used to transfer information off of the device. If the application is asking for access to the network, you should ask yourself whether the application needs that access to perform its intended task. If it doesn't, the application could be putting the network at inappropriate or unnecessary risk. If you need assistance in making this determination, you should contact your MISO. 		
6.	Are you aware of any concerns about the application's reputation?		

Ask yourself		Yes	No
	<ul style="list-style-type: none"> For example, some application stores or providers (e.g., Android) do not currently vet their applications to the same degree as others. While this does not mean that these applications are not safe or suitable (to the contrary, many of these applications are perfectly safe and useful), it may, at least for the near future, warrant some additional consideration. <p>Note: if you have no information on the reputation of the application or its manufacturer, the following sources may help:</p> <ul style="list-style-type: none"> Do an internet search of the application and the manufacturer Check out user reviews of the application Ask your colleagues or Ministry Information Security Officer 		
7.	<p>Is there anything about the application or software, not already addressed above, that concerns you?</p> <ul style="list-style-type: none"> Services available on devices and the threats to devices, privacy and information change all the time and cannot all be addressed in a guidance document such as this. For this reason, if there is anything about the application or software that concerns you or makes you uncomfortable, you should seek advice from your Ministry Information Security Officer. 		

Further Considerations:

Generally speaking, it is good practice to remove old applications and software from your device when you are no longer using them. This helps the device to run more efficiently, and also helps ensure that the minimal amount of information that is needed is accessed.

For information about the Appropriate Use Policy contact:

Information Stewardship and Policy Branch
lm.itpolicy@gov.bc.ca

