BCNET
Shared Services for Higher Education & Research

Privacy Impact Assessment: TelemetryTV

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	TelemetryTV
Organization:	BCNET
Branch or unit:	
Your name and title:	Jarod Hooper, Privacy Consultant Hooper Access and Privacy Consulting Ltd.
Your work phone:	250-588-8055
Your email:	jarod@hooperconsulting.ca

Initiative Lead name and title:	Devon Keys, Senior Business Analyst Shared Systems and Technology
Initiative Lead phone:	604-343-0506
Initiative Lead email:	devon.keys@bc.net
Privacy Officer:	
Privacy Officer phone:	
Privacy Officer email:	

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No.
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No.
Related PIAs, if any:
BCNET has completed a PIA on AWS (Canada) which can be referred to for additional information.

1. What is the initiative?

BCNET is a federally incorporated not-for profit services and information technology organization that represents the interests of its member institutions comprised of 25 publicly funded universities, colleges, institutes, and research organizations across British Columbia. It represents all public, post-secondary education institutions in the province and provides shared services to its members in the areas of networks, procurements, licensing, and IT services.

BCNET is assessing TelemetryTV, a service sold by Microserve, on behalf of its member institutions. TelemetryTV is a digital signage platform that delivers brand compliant content through an intuitive secure platform allowing for more engaging, collaborative, and time-efficient digital communications.

TelemetryTV hosts a library of 70+ turn-key applications allowing the user to curate unique multimedia content. TelemetryTV offers a robust set of user and playlist permission settings. These playlist settings include scheduling rules that will automatically remove expired content, restrict or enable content on specific devices, and allow update or review by any approved user.

2. What is the scope of the PIA?

This PIA addresses the collection, use, disclosure, storage, access, and security of personal information in TelemetryTV's digital signage platform.

3. What are the data or information elements involved in your initiative?

The data elements involved are cookies and usage data, as well as text, photographs and/or videos used in content creation that may contain information/images of identifiable individuals. The usage data and cookies include information such as each user's computer Internet Protocol address (IP address), browser type, browser version, the pages of the service that are visited, the time and date of the visit, the time spent on those pages, unique device identifiers and other diagnostic data.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

N/A.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 1: Usage data is collected by TelemetryTV when users access the platform. Photographs/videos are collected by institutions for content creation.	Collection	26(a), 26(d)	
Step 2: Usage data and cookies used by TelemetryTV include information such as each user's computer Internet Protocol address (IP address), browser type, browser version, the pages of the service that are visited, the time and date of the visit, the time spent on those pages, unique device identifiers and other diagnostic data. Media will be uploaded into TelemetryTV	Use	32(b)	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FOIPPA authority	Other legal authority
for use in content creation which may also include text identifiers.			
Step 3: Distribution of content.	Disclosure	33(2)(c)	

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

BCNET member organizations are responsible for ensuring the appropriate notification is in place prior to the collection of personal information.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

No.

8. Does your initiative involve sensitive personal information?

Yes.

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

- If yes, go to question 10
- If no, go to Part 4

10. Where are you storing the personal information involved in your initiative?

After you answer this question go to Part 5.

Personal information is stored in data centres located in Canada.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

11. Is the sensitive personal information stored by a service provider?

N/A.

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

N/A.

13. Does the contract you rely on include privacy-related terms?

N/A.

- If yes, describe the contractual measures related to your initiative.

15. What controls are in place to prevent unauthorized access to sensitive personal information?

N/A.

16. Provide details about how you will track access to sensitive personal information.

N/A.

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.
N/A.					

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

18. Does your initiative involve digital tools, databases or information systems?

Yes.

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

No.

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. What technical and physical security do you have in place to protect personal information?

BCNET

BCNET member institutions are responsible for ensuring the physical security of all data while in their custody and/or control (including data at rest or in transit) and must meet applicable physical security standards required by their organization.

BCNET member institutions are responsible for ensuring the technical security of all data in their custody and/or control (including data at rest or in transit) and must meet applicable technical security standards required by their organization.

TelemetryTV

Section 21, Section 15(1)(l)

20. Controlling and tracking access

BCNET member institutions are responsible for controlling and tracking access to the personal information.

Strategy - TelemetryTV	
We only allow employees in certain roles access to information	Yes
Employees that need standing or recurring access to personal information must be approved by executive lead	Yes

Strategy - TelemetryTV	
We use audit logs to see who accesses a file and when	Yes
Describe any additional controls:	TelemetryTV allows authenticated users to control and limit access to other users accessing the service. Authenticated users can also view detailed log reports of each user's activity on that account.

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

Member institutions must provide proper documentation to protect the privacy of individuals who may be featured in media used in content creation.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

Member institutions are responsible for ensuring personal information involved in media is accurate and complete after consent. Member institutions are also responsible for correcting personal information.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

N/A. See above.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A. See above.

23. Does your initiative use personal information to make decisions that directly affect an individual?

No.

- If yes, go to question 25
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

N/A.

- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement?

No.

- If yes, please complete the Information Sharing Agreement Supplement and attach it to your PIA.

26. Will your initiative result in a personal information bank?

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

No.

- If yes, please complete the table below.

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the PIB

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

27. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Add new rows if necessary.

Possible risk	Response
Risk 1: Employees of BCNET or member institutions access personal information and use or disclose it for unauthorized purposes.	Access will be restricted to only those who require access to support the program. Each member institution is responsible for ensuring confidentiality and adequate risk mitigation tools are in place.
Risk 2: Employees of TelemetryTV access personal information and use or disclose it for unauthorized purposes.	Section 21, Section 15(1)(l)
Risk 3: Media is compromised during transmission to TelemetryTV.	The BCNET member institution is responsible for ensuring that transmission occurs via a secure and approved process.

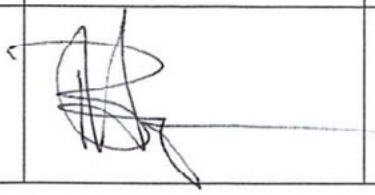
PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Consultant	Bev Hooper, Hooper Access and Privacy Consulting Ltd.		March 22

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Program/Department Manager	Dean Crawford, Director, Shared Systems and Technology	Dean Crawford	Mar 2, 2022
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate Only required if personal information is involved	Bala Kathiresan, President and Chief Executive Officer		Mar 2, 2022