IN THE MATTER OF

FORTISBC ENERGY UTILITIES

APPLICATION FOR REMOVAL OF THE RESTRICTION ON THE LOCATION OF DATA SERVERS PROVIDING SERVICE TO THE FEU, CURRENTLY RESTRICTED TO CANADA

DECISION

October 13, 2015

BEFORE:

L. A. O'Hara, Panel Chair/Commissioner
N. E. MacMurchy, Commissioner
K. A. Keilty, Commissioner

TABLE OF CONTENTS

Page No.

EXECUTIVE SUMMARY

This decision addresses an application by FortisBC Energy Utilities (FEU) for the removal of a restriction on the location of FEU's data and servers. FEU are currently restricted from locating their data and servers outside of Canada unless the Commission consents to a specific application by FEU to do so. FEU's application is to remove the restriction but include a requirement that specific data be encrypted or de-identified, as a security and privacy measure, if stored outside of Canada and that the keys to the encryption and de-identification would be stored in Canada.

The Commission approves FEU's request subject to the company remaining a Canadian owned and controlled company located in Canada.

To arrive at this determination, the Panel focused on the differences between the status quo under the current restriction and the FEU application. The Panel considered FEU's application pursuant to section 44 of the *Utilities Commission Act* and used a benefit-risk assessment to determine whether the proposal is in the public interest.

The potential benefits of storing data outside of Canada are cost savings and access to services that are not stored on servers in Canada. The potential risks are that the data is accessed by those who, for privacy and security reasons, should not have access to the data or for whom the owner of the data has not granted consent. These risks are typically unauthorized access and authorized foreign government access. Unauthorized access can occur through hacking or unauthorized employee, insider, contractor or third party vendor access. Authorized foreign government access can occur because data are subject to the laws of the jurisdiction in which they are held; a foreign government may therefore lawfully access data held on servers in its jurisdiction.

In its benefit-risk assessment, the Panel finds there are potential benefits to FEU and their ratepayers if the restriction is lifted because removal of the restriction would allow access to a number of service providers who can potentially provide cost savings. While the potential benefits could be pursued under the status quo, the Panel recognizes the benefit of reduced regulatory costs if FEU are not required to file individual applications for specific projects. Furthermore, the Panel finds that the pursuit of cost savings is consistent with the Performance Ratemaking Plan which FEU is currently under.

With regard to the risks and, specifically regarding unauthorized access, the Panel accepts the characterization that the digital universe has no borders. Therefore, in the Panel's view, the risk of unauthorized access is not related to location of the data. Rather, it is related to how comprehensive the data security and privacy regimes are. In the Panel's view, FEU's security and privacy regime is adequate to mitigate the risk of unauthorized access.

Regarding the risk of authorized foreign government access, all parties in this proceeding agree that this risk exists because data is subject to the laws of the jurisdiction in which it is stored. FEU's primary mitigation strategy against this risk is encrypting and de-identifying personal, customer and sensitive data that is stored outside of Canada and keeping the encryption and de-identification keys in Canada. Encryption and de-identification is so difficult to break without the keys that the relevant consideration for this risk assessment is whether a foreign government can compel the provision of keys stored by FEU in Canada through the foreign judicial system.

The Panel accepts FEU's assessment that under the principles of international law a foreign authority may not legally compel FEU, which are owned and controlled by a Canadian company, to provide encryption and/or de-identification keys, unless ordered to do so by the Canadian court. The key factor of this protection, however, is that FEU are Canadian owned and controlled by their parent company, Fortis Inc. which is located in Canada.

In conclusion, given that the risks of data being stored outside of Canada are adequately mitigated, the Panel considers that it is in the public interest for FEU to be given the opportunity to pursue the potential benefits. The Panel approves FEU's application subject to the company continuing to be owned and controlled by a Canadian company located in Canada.

The Panel finds that some level of reporting is warranted to enable the Commission and participants in this proceeding to monitor the outcomes of this decision. Accordingly, FEU are directed to file an annual report detailing any significant security and/or privacy breaches and the associated resolution process, and any significant deficiencies identified in processes and controls and the associated remediation process.

1.0 INTRODUCTION

1.1 The Application

On August 1, 2014, FortisBC Energy Utilities (FEU, also referred to as FEI in this decision)[1] filed an application with the British Columbia Utilities Commission (Commission) for the removal of a restriction on the location of FEU's data and servers (Application). The current restriction states:

> [T]he Commission orders that the location of data and servers providing service to the [FEU] is to be restricted to Canada and that any proposal to locate data and servers providing services to the [FEU] (including data and servers providing back-up services) outside Canada will require the Commission's approval.[2]

Through the course of the proceeding FEU altered their application to request the Commission remove the restriction on the location of data and servers but include provisions to protect personal information about customers by way of encryption or de-identification if the information is stored outside of Canada. This proposed alternative relief was further modified to include wording to protect customer, employee, and sensitive information.[3]

FEU submitted the application because they believe that continuing to restrict the location of data and servers is no longer necessary and practical. FEU proposed the alternative relief to address concerns raised in the proceeding regarding privacy and security of certain information.[4]

1.2 Approval sought

As mentioned above, as the hearing progressed, the approval sought by FEU evolved to the request below:[5]

(a) Effective the date of this order, the restriction imposed under Orders G-116-05, G-75-06 and G-49-07 that the location of data and servers providing service to FEI be restricted to Canada, is removed and no longer in effect.

(b) For the purposes of this order:
- "**Customer Information**" means information of or about the FEI residential, commercial, or industrial customers.
- "**Employee Information**" means information of or about the FEI employees.

---

[1] While FEU were the original applicant in this proceeding, the companies that comprised FEU were amalgamated on December 31, 2014 and the amalgamated entity carries on business under the name FEI (FortisBC Energy Inc.). Evidence and submissions were made in this proceeding using both names, FEU and FEI. For the purpose of this decision, FEU and FEI are used interchangeably.

[2] Commission Order G-75-06.

[3] Exhibit A-11, Order G-26-15; Transcript Volume 2, p. 78.

[4] FEU December 18, 2014 Reply Submission, p. 9.

[5] FEU June 30, 2015 Final Submission, pp. 4–5.

- "**Sensitive Information**" includes:
  - financial, commercial, scientific or technical information, the disclosure of which could result in undue financial harm or prejudice to FEI; and
  - information that relates to the security of the FEI critical infrastructure and operations, the disclosure of which could pose a potential threat to the FEI operations or create or increase the risk of a debilitating impact on the safe and reliable operation of the FEI system.
- "**Encrypted**" means an encryption methodology using current industry standards for secure encryption.
- "**De-identified**" means a de-identification methodology consistent with current industry practice for the purpose of protecting personal information.
- "**Encryption keys**" and "**De-identification keys**" mean any information or methodology used to access encrypted or de-identified data.

(c) Effective as the date of this Order, FEI is permitted to store data on servers located outside of Canada, provided that data containing **Customer Information, Employee Information,** or **Sensitive Information,** or any combination thereof, must be either **Encrypted** or **De-identified** if such data is to be stored on servers located outside of Canada.

(d) **Encryption keys** and **De-identification keys** for **Encrypted** or **De-identified** FEI data stored outside of Canada must be stored on servers located within FEI's data centres that are located in Canada.

This request was referred to as the modified alternative relief throughout the proceeding. In this decision, for ease of reading, it is referred to as FEU's updated proposal.

1.3 Hearing process

The application was heard by way of written hearing and streamlined review process. There were three registered interveners in the hearing: B.C. Sustainable Energy Association and the Sierra Club British Columbia (BCSEA); the Commercial Energy Consumers Association of British Columbia (CEC); and the British Columbia Old Age Pensioners' Organization, *et al.* (BCOAPO). One party registered as an interested party but was not an active participant. No letters of comment were received despite the Commission requiring public notice for this proceeding.

2.0 PAST DECISIONS AND LEGISLATIVE FRAMEWORK

2.1 History

2.1.1 Kinder Morgan Inc. decision and clarification

The restriction was originally created by Commission Order G-116-05 after a proceeding on *The Matter of An Application by Kinder Morgan Inc. and 0731297 B.C. Ltd. for Approval of the Acquisition of the Common Shares of Terasen Inc.* That proceeding was for Kinder Morgan Inc. (KMI), a U.S. energy storage and transportation company, to acquire the common shares of Terasen Gas Inc. (Terasen), a Canadian company, such that KMI would have indirect control of Terasen.

In that proceeding the public raised concerns about the application by way of over 8,000 letters of comment to the Commission.[6] One specific concern raised related to the U.S. Patriot Act and the potential for the privacy of British Columbians to be violated under that Act if Terasen's billing and record keeping functions were relocated to the U.S.[7]

At the close of that proceeding the Commission approved the application and KMI's acquisition of common shares subject to certain conditions including a condition that KMI was not to change the geographic location of any existing "functions"[8] or data currently in Terasen's service area without prior approval of the Commission. The Commission imposed this condition to address concerns raised in the proceeding about privacy, gas procurement and other critical functions.[9]

2.1.2 Fortis Inc. acquisition of KMI shares

On March 1, 2007, Fortis Inc. applied to the Commission to acquire the issued and outstanding shares of Terasen from KMI. In that application Fortis Inc. stated that it would accept the data restriction in place for KMI. The Commission approved Fortis Inc.'s application subject to the restriction on the location of functions and data that was imposed on KMI.[10]

2.1.3 Current mechanism for re-locating data

The current restriction on the location of FEU's data and servers states that "any proposal to locate data and servers providing services to the [FEU]…outside Canada will require the Commission's approval."[11]
FEU applied for and was granted an exception to the restriction for a specific project in the past.[12] On August 21, 2006, FEU filed an application with the Commission seeking to maintain their process and control documentation required for Ontario Securities Commission compliance on KMI's licensed software and to allow internal audit staff to store electronic document files on a shared server owned by KMI and located in Houston, Texas.[13] The Commission approved the 2006 application by Order G-112-06.

---

[6] *In the Matter of an Application by Kinder Morgan, Inc. and 0731297 B.C. Ltd. For the Acquisition of Common Shares of Terasen Inc.,* Decision, November 10, 2005, p. 13.
[7] Ibid., p. 20.
[8] By way of Letter L-30-06 and Order G-75-06 the Commission clarified "functions" to include all functions performed by Terasen Inc. for Terasen Utilities including corporate services and operations such as Human Resources, Gas Supply, Marketing, etc. and clarified that the location of the data is determined by the location of the server.
[9] Ibid., p. 39.
[10] *In the Matter of Fortis Inc. Application for Approval of the Acquisition of the Issued and Outstanding Shares of Terasen Inc.,* Reasons for Decision, Appendix A to Order G-49-07, April 30, 2007, p. 15.
[11] Commission Order G-75-06.
[12] Exhibit B-3, BCUC IR 1.1.1.
[13] Ibid., BCUC IR 1.1.1.1.

2.2 *Utilities Commission Act* – Section 44 Duty to keep records

Section 44 of the *Utilities Commission Act* (UCA) is the only section of the statute that deals specifically with the location of a public utility's records. It states:

> "Duty to keep records
>
> **44** (1) A public utility must have in British Columbia an office in which it must keep all accounts and records required by the commission to be kept in British Columbia.
>
> (2) A public utility must not remove or permit to be removed from British Columbia an account or record required to be kept under subsection (1), except on conditions specified by the commission."

3.0 DECISION FRAMEWORK

This Application is a request for a change from the status quo, where FEU are restricted from locating their data and servers outside of Canada unless the Commission consents to a specific application for the company to do so. FEU's updated proposal requests that FEU could locate their data and servers outside of Canada, except for certain data which would have to be encrypted or de-identified but the keys to the encryption and de-identification would have to be kept inside Canada. Given the nature of this request the Panel has focused on the differences between the status quo and the updated proposal. To do this, the Panel will first address FEU's rationale to remove the current restriction, and then move on to a benefit-risk assessment where the Panel will identify and focus on the benefits and risks of the updated proposal as compared to the status quo. The Panel will weigh the benefits against the risks to determine if the updated proposal should be granted.

The Panel will consider the updated proposal pursuant to section 44 of the UCA, and, using the aforementioned benefit-risk assessment, will determine if the updated proposal is in the public interest.[14]

3.1 FEU reasons to remove current restriction

FEU believe that continuing to restrict the location of data and servers is no longer necessary and practical for reasons including:

- British Columbia's private sector privacy regulation has evolved considerably since 2005 when the data restriction was first put in place;
- the original basis for the data restriction, which was largely due to the fact that the then Terasen companies were being acquired up by KMI, a U.S. company, no longer exists because FEU are Canadian owned utilities;
- technology has advanced since 2005 and customers should benefit; and
- the data restriction limits the ability of FEU and FortisBC Inc. to integrate systems, which limits benefits to the customers of both companies. [15]

---

[14] Although the current restriction was imposed under section 54(9) of the UCA which involves reviewable interests, section 54(9) does not apply in this proceeding as there is no transfer of shares.

[15] Exhibit B-4, p. 3; FEU December 4, 2014 Final Submission, p. 1.

FEU explained that removal of the current restriction would allow FEU to consider technology and services to serve customers efficiently and cost effectively, for example, through third party vendors which store data or provide services. FEU's view is that there is no increase in risk associated with the location in which data is stored and that they have experience and expertise to protect their systems and information through appropriate controls around security and privacy.[16]

3.2 Details of FEU's updated proposal

In their updated proposal, FEU propose that certain information be encrypted or de-identified if stored outside of Canada.

Encryption is the process of encoding information or data in such a way that only authorized parties can read it. FEU rely on "Advanced Encryption Standards" (AES) as the basis for encrypting. FEU's Director of Information Systems explained:

> Encryption uses an algorithm to randomize data to transmit or store outside of FortisBC. Encryption makes data unrecognizable and unusable without a decryption key, which we keep within our FortisBC data centres… FortisBC uses the current industry standard, 256 bit advanced encryption, to protect our data… it is considered fundamentally impossible to decrypt information encrypted using the methodologies that FortisBC uses, without the key.[17]

FEU submit they have been using encryption for many years within Canada to allow external access to company information for customers, vendors and employees.[18] In general, FEU currently use encryption for data that is stored outside of FEU's data centers when the data is not needed to be recognized by parties outside of FEU.[19] FEU estimate the cost of a dedicated AES encryption server as a one-time cost of $10,000 plus $50 annual cost per encryption key. Most information technology services would require 3 keys.[20]

De-identification, such as tokenization and field removal, is the removal of information from a data set which connects a person's identity to the data set. Tokenization is a de-identification method to replace sensitive information with random information.[21] Field removal uses a database script to completely remove targeted fields containing, for example personal information from a data set.

FEU use de-identification to send data, without encrypting, for purposes of analysis or collaboration with vendors or other industry groups.[22]

---

[16] Transcript Volume 2, p. 75.
[17] Ibid., pp. 62, 64.
[18] Exhibit B-8, pp. 2–3; Exhibit B-9, Alternative Relief BCUC IR.1.6.1.
[19] Transcript Volume 2, p. 62.
[20] Exhibit B-11, Alternative Relief BCSEA IR 1.15.1.
[21] Exhibit B-8, p. 5.
[22] Transcript Volume 2, p. 64.

FEU estimated that a field removal solution would cost approximately $50,000. If tokenized information needs to be de-tokenized, a key table or index needs to be maintained to re-establish the tokenized data to its original form. FEU estimated that a product that can de-tokenize will cost approximately $250,000 as a one-time installation cost and annual support for licensing will cost approximately $20,000.[23]

4.0 IDENTIFICATION OF POTENTIAL BENEFITS

BCSEA, BCOAPO, and CEC all raise a concern that FEU's application lacks details regarding potential benefits.[24] FEU submit that they currently do not have specific plans to use any technology systems or store data outside of Canada.[25] FEU state that "[t]he Commission should not lose sight of the overarching rationale of allowing the FEU to explore, pursue and implement opportunities that can benefit customers."[26]

FEU submit that removing the restriction would allow FEU to consider and select information systems, service providers and software which will provide the greatest value and benefits for customers without li miting the selection process based on location.[27]

In response to the interveners' concerns about the lack of detail of benefits, FEU provided examples of a number of potential projects they may pursue:[28]

Project Description	Potential Savings
Microsoft Azure – storage and infrastructure service hosted on servers in Microsoft data centres in the United States.	Reduce approximately $100,000 annual operating costs.
Microsoft Office 365 – desktop computing, user storage, Exchange services with email servers and storage, SharePoint services and Lync communication tools.	Operational savings of approximately $250,000 per year.
Human Resource Management system – improve functionality around talent management, attendance management, reporting and other HR functions.	Save approximately $1 million in capital and $200,000 to $400,000 annually in operating expense.
Tools for managing energy usage – off-the-shelf solutions that are hosted outside of Canada, such as Opower or Itron.	Not provided by FEU.
Portfolio Manager – FEU providing consumption data to the benchmarking tool for energy efficiency of commercial buildings.	Not provided by FEU.

[23] Exhibit B-9, Alternative Relief BCUC IR 1.9.4.1.
[24] BCOAPO December 10, 2014 Final Submission, pp. 1, 6; CEC December 11, 2014 Final Submission, pp. 2–3, 5, 7–9; Transcript Volume 2, pp. 19–20, 27, 31.
[25] Exhibit B-3, BCUC IR 1.2.2–1.2.7.
[26] Exhibit B-13, p. 3; FEU August 4, 2015 Reply Submission, p. 7.
[27] Exhibit B-6, CEC IR 1.6.1, 1.4.4.
[28] Exhibit B-8, pp. 12–15; Transcript Volume 2, pp. 66–70.

4.1 Submissions by the parties

BCOAPO submits that the details of benefits to the customer are "not well developed in the Application or in subsequent submissions made by the FEU… Not enough information is provided on these benefits and the costs of accessing them with the restrictions in the proposed relief…in order to assess whether it is actually a benefit to ratepayers."[29]

BCOAPO further submits that the current restriction does not prohibit FEU from applying to the Commission with a specific proposal to locate data or servers outside of Canada.[30]

BCSEA submits that the current data restriction does not prevent FEU from implementing cost saving technology because FEU may request Commission approval to locate data outside of Canada, which they have been successful with in the past.[31]

On the other hand, CEC states that "there is a potential for cost savings or productivity improvements in storing data outside Canada, and there is likely no significant impact on customer costs to encrypting or de-identifying information."[32]

FEU submit that the application is general and not directed at a specific project. While the current restriction includes a mechanism for FEU to locate data and servers outside of Canada by applying to the Commission for approval of specific proposals on a case-by-case basis, FEU submit that the current mechanism results in regulatory inefficiency and increased regulatory cost.[33] FEU believe that it would not be practical, efficient or cost-effective to bring forward discrete applications for exemption and that the cost savings from a potential project would be "eaten up" by the time and cost to prepare an application to the Commission for the project.[34]

FEU further state "[t]he validity of the FEU's description of the quantum of the benefits has not been questioned or challenged in this proceeding, and the FEU submit that there is no good reason to doubt that such benefits can be achieved for the benefit of customers."[35]

4.2 Panel discussion and determination

While analysis of the benefits would be more straightforward if dealing with a specific proposal, the Panel acknowledges that FEU have no specific plans at this point and therefore the Panel must evaluate FEU's evidence on *potential* benefits. The question for the Panel thus becomes whether there is a potential for FEU and their ratepayers to achieve meaningful benefits if the restriction on data and server location is removed.

---

[29] BCOAPO July 27, 2015 Final Submission, p. 5.
[30] Ibid., p. 8.
[31] BCSEA December 11, 2014 Final Submission, p. 4.
[32] CEC July 27, 2015 Final Submission, p. 10.
[33] Exhibit B-3, IR 1.1.
[34] Exhibit B-13, p. 4; Transcript Volume 2, pp. 53–54, 73–74.
[35] FEU August 4, 2015 Reply Submission, p. 8.

The Panel finds that there are potential benefits to FEU and their ratepayers if the current restriction is removed. The potential benefits exist because as demonstrated by FEU's potential projects, removing the restriction on data and server location would allow access to a number of service providers who can potentially provide cost savings. While these potential benefits could be pursued under the current mechanism, the Panel recognizes the benefit of reduced regulatory costs if FEU are not required to make individual applications to store data on servers located outside of Canada. The Panel also notes that these potential benefits exist net of the cost of encryption and de-identification.

The Panel also notes that a Multi-year Performance Rate Making Plan for 2014-2018 was approved for FEU in 2014. The objective of the plan is to provide FEU with an incentive to reduce costs. Cost savings that result from projects, such as those described by FEU in this proceeding, that reduce operations and maintenance costs, will flow through to both the FEU shareholder and the FEU customer. Pursuit of such savings is consistent with the logic behind the granting of the Performance Rate Making plan.

Given the finding on potential benefits, the Panel will now identify the potential risks and assess FEU's risk mitigation strategies before weighing these risks against the potential benefits in its final determination.

5.0 IDENTIFICATION OF POTENTIAL RISKS

The general risks of storing data are that the data is accessed by those who, for privacy and security reasons, should not have access to the data or for whom the owner of the data has not consented to access. These risks are generally of two types: unauthorized access and authorized foreign government access.

5.1 Unauthorized access

Unauthorized access to data can occur through means such as hacking or unauthorized employee, insider, contractor or third party vendor access.
FEU submit that the storage of data outside of Canada does not increase the risk of unauthorized access to that data, because:

> First, FortisBC uses the same security protocols, procedures, policies, assessments, and requirements no matter where data is stored. In addition, FortisBC is still subject to the same British Columbia and Canadian privacy legislation regardless of where it chooses to store data and will still be held accountable in exactly the same way.
>
> Secondly, the digital universe has no borders. In other words, if a person wanted to gain unauthorized access to data, that person could be located anywhere in the world, and the location of the data itself would not change that fact… In the unlikely event of a breach of that data, it wouldn't be protected by borders.[36]

[36] Transcript Volume 2, pp. 56–57.

Questions were raised during the proceeding as to whether one country would have greater unauthorized access risk than another. FEU indicate that they would evaluate the risk of a particular jurisdiction or country at the vendor level by assessing the specific practices, policies and processes of a third party vendor against the sensitivity and volume of personal information which would be disclosed and then would only contract with a vendor if it could meet FEU's security requirements.[37,]

5.2 Authorized foreign government access

FEU confirmed that if data and servers are stored outside of Canada they may be subject to the laws of the jurisdiction in which they are held.[38] FEU explain two types of authorized foreign government access risk related to their updated proposal:

> The first aspect is the risk that a foreign government seizes data in the hands of a foreign third party vendor with whom the FEU store data….[t]he second aspect of this risk is the risk of a foreign government being able to directly seize an encryption key from the FEU within Canada … this is not a risk in the case of the FEU because it is a Canadian owned and controlled company … Under the principles of international law, a foreign court cannot simply reach across the Canadian border to order the FEU to provide an encryption key…[39]

Regarding the risk of a foreign government seizing an encryption key from FEU within Canada, FEU state they are neither American companies nor foreign subsidiaries of an American company[40] and submit a letter from the Information and Privacy Commissioner for British Columbia which states:

> …personal information stored in Canada may be accessed by foreign governments where a company that has custody or control of the personal information is a subsidiary of a foreign company or otherwise amenable to the jurisdiction of a foreign court. A foreign court or government that is authorized by legislation or a rule of court may order a company that is subject to its jurisdiction to produce records even where the information is located in a different country. This principle could in theory apply to enable access to the [de-identification key] itself. Generally, whether a foreign company could be compelled to provide access to a record will depend upon the actual ability of the company to obtain the information. While it is likely that a foreign court will balance the interests of both states where a Canadian statute…would preclude disclosure, it is also likely that foreign interests will outweigh Canadian interests where national security or public safety are said to be at issue.[41]

---

[37] Transcript Volume 2, pp. 142–144, 71.
[38] Exhibit B-3, BCUC IR 1.4.1; FEU June 30, 2015 Final Submission, pp. 5–8.
[39] Transcript Volume 2, p. 57; FEU June 30, 2015 Final Submission, pp. 6–7.
[40] Exhibit B-11, Alternative Relief BCSEA IR 1.17.2.
[41] Exhibit B-8, p. 8; Appendix D, pp. 5–6.

5.3 Risk mitigation strategies

FEU provided evidence on a number of strategies it uses to mitigate risks associated with locating data and servers outside of Canada including the encryption and de-identification of data, vendor due diligence, and security and privacy impact assessments. As well, FEU's position is that the BC privacy regime itself has evolved since 2006 to create laws that require FEU to protect data and mitigate risk anywhere data is stored.

5.3.1 Encryption and de-identification

Under the updated proposal data would be encrypted prior to exiting the FEU data centres and network. FEU's evidence is that the encryption methodology used by the FEU has never been compromised.[42] However, FEU acknowledge that "to say there is zero risk is impossible" but "fundamentally it is impossible to decrypt data. There's not enough computing power on this planet to decrypt it within any reasonable amount of time, without the keys."[43] Based on the strength of the encryption and de-identification methods, FEU submit that if security were breached, "whether by a hacker or other means, any compromised data would be unusable, unidentifiable, and undecipherable."[44]

FEU submit that the primary risk to encrypted and de-identified data is access to the keys required for decryption or re-identification. FEU submits that keys would be held within the FEU, and access to those keys would be restricted to a limited number of employees called Domain Administrators. Domain Administrator activity is audited internally as well as by an independent third party on an annual basis.[45]

With respect to managing FEU employee access to keys, FEU explain:

> It comes down to your controls around access privilege, in which case every access is authorized, depending on the person's role in the organization, or the contractor's role for us. It's granted on an individual basis and it's role based and it's based on access of least privilege… The whole intention of controlling access to system is to ensure that no one individual can materially damage or access information, all information.[46]

FEU state that employees with access to the keys have undergone security checks such as reference, background, and criminal record checks prior to hiring.[47]

Specifically for tokenization, FEU submit that if information is tokenized and re-identification is not required, no key is retained. FEU state that this almost eliminates the risk of the de-identified information being re-identified.[48]

---

[42] Transcript Volume 2, p. 129.
[43] Ibid., pp. 129–130.
[44] Transcript Volume 2, pp. 64–65; Exhibit B-8, pp. 2–3.
[45] Ibid., p. 4.
[46] Transcript Volume 2, pp. 160–161.
[47] Exhibit B-6, CEC IR 1.15.
[48] Exhibit B-8, p. 7.

5.3.2 Security assessment

FEU would complete a security risk assessment on all projects which involve encryption and de-identification.[49] These assessments consider factors including viability of third party vendors, organizational breakdown, types and versions of firewalls and malware protection, infrastructure evaluation, guarantees of access control, quarterly audits, reference checks, backup procedures and disaster recovery capabilities.[50] FEU described their security risk assessments as prescriptive with non-negotiable requirements. FEU submit that a potential project will not proceed if a vendor fails any part of FEU's security assessment and that the security assessment ensures that any potential risks are addressed regardless of where the data is located.[51] Furthermore, FEU state that "[w]e don't allow for any sort of flexibility in our requirements. It doesn't matter what culture or what country is managing our data, our information, they have to adhere to those requirements."[52]

FEU review their security assessment program annually to account for technology changes and internal controls are reviewed by third parties on an annual basis.[53] Controls are reviewed on a regular basis by internal and external audit.[54] FEU submit that independent third party security experts test and report on the effectiveness of FEU's methods and technology.[55] The scope of testing work includes attempts to penetrate FEU's internal systems, evaluation of access points in FEU's websites and access levels to hosted environments, and review of change control protocol and versions of security testing.[56]

FEU provided evidence that "… we base our risk assessments on industry standards. Our risk assessments are tested through auditors to ensure they're acceptable, and we do not plan on increasing our risk tolerance just to store data somewhere else… We won't accept additional risk just to save money."[57]

5.3.3 Privacy assessment

According to FEU's Chief Privacy Officer, following a security assessment, FEU determine whether a project involves the collection, use or disclosure of personal information and if so, FEU perform a privacy impact assessment.[58]

FEU submit that a privacy impact assessment seeks to identify and evaluate any privacy related risks associated with the collection, use, disclosure, security and retention of personal information.[59] The privacy impact assessment asks questions to identify the privacy risks and determine ways to mitigate those risks.

---

[49] Exhibit B-11, Alternative Relief BCSEA IR 1.20.1.
[50] Exhibit B-12, Alternative Relief CEC IR 1.1.3.
[51] Transcript Volume 2, p. 148.
[52] Ibid., p. 140.
[53] Ibid., p. 150.
[54] Ibid., p. 153.
[55] Transcript Volume 2, p. 63.
[56] Ibid., p. 177; Exhibit B-9, Alternative Relief BCUC IR 1.7.3; Exhibit B-12, Alternative Relief CEC IR 1.1.3.
[57] Ibid., p. 131.
[58] Transcript Volume 2, pp. 71–72.
[59] Exhibit B-12, Alternative Relief CEC IR 1.1.2.

FEU state that "[i]t's not an assessment of how much additional risk are we willing to take. It's an assessment of how do we maintain the high level of security and rigour that we have around our data today."[60]

FEU submit that "if a privacy assessment is completed and the privacy risks that have been identified cannot be appropriately mitigated, the project will not move forward."[61]

5.3.4 Third-party vendor selection and contractual provisions

FEU described their vendor selection process and controls as follow:

> [The]due diligence process…can include (if appropriate) background checks, reference checks and assessments completed by independent third parties. For instance, for major information systems initiatives, a recognized technology consultant will often be retained to assist in assessing a particular vendor. Finally, there are contractual terms in agreements with vendors which would help to mitigate any privacy or security risks that may be identified as part of the due diligence process by including representations, covenants, and insurance and indemnity provisions.[62]

FEU submit that third party vendors must comply with FEU's security requirements including:

- using security tools such as firewalls and anti-malware software;
- using access controls including logical access controls to ensure a minimum number of people have access to the systems or infrastructure housing FEU data, and audits of access logs which are reviewed by FEU;
- having a documented incident management program and maintenance schedule; and
- providing adequate training for vendor staff.[63]

FEU submit that they review and test vendors' compliance with FEU's requirements and that "an organization's inability to comply with any one of [FEU]'s security requirements would make them ineligible to provide service to [FEU]. Costs do not override requirements."[64] FEU also indicate that the same level of security requirements is used regardless of where the data is stored and the decision as to whether to proceed with a certain vendor would be based on the results of the risk assessment and would ensure that the FEU are able to get appropriate contractual provisions in place to minimize any risks identified.[65]

5.3.5 BC's private sector privacy regulation

While not a mitigation strategy employed by FEU, the evolution of the laws and policies around privacy in British Columbia must be explored as FEU have submitted that this evolution supports their updated proposal.

---

[60] Transcript Volume 2, p. 146.
[61] Ibid., p. 74.
[62] Exhibit B-3, BCUC IR 1.3.4.1.
[63] Transcript Volume 2, pp. 66–71.
[64] Ibid., p. 71.
[65] Exhibit B-6, CEC IR.1.1.6; Transcript Volume 2, pp. 57, 139.

In FEU's view, the privacy regime in British Columbia is much different than it was in 2006 when the current restriction was imposed. FEU submit that the current privacy regime is far more robust, privacy awareness is much more prevalent, and there is an abundance of case law and guidance from the British Columbia Office of the Information and Privacy Commissioner and the federal Office of the Privacy Commission that has come into being since 2006. FEU also have a published privacy policy that sets forth their commitment to privacy protection, and outlines the purposes and limited scope under which personal information is generally collected, used and disclosed.[66] FEU believe that the provincial and federal privacy legislation and framework in place today, along with FEU's privacy policy, sufficiently address any and all privacy concerns, including those that were raised in initial proceedings that led to the creation of the restriction.[67]

In terms of storing data outside of Canada, FEU submit that under Canada's private sector privacy legislation, an organization remains accountable for the "personal information" that it collects, uses and discloses, even if it stores that information outside of Canada.

FEU cite section 4(2) of British Columbia's *Personal Information Privacy Act* (PIPA) and section 4.1.3 of Canada's *The Personal Information Protection and Electronic Documents Act* (PIPEDA), which respectively state:

> An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization.
>
> An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.[68]

FEU state that "PIPA and PIPEDA will be enforceable against the FEU for personal information collected, used or disclosed on our behalf regardless of what jurisdiction we retain a third party contractor in."[69]

FEU contractually obligate vendors who have access to personal information to comply with British Columbia and Canadian privacy laws.[70]

5.3.6 General submissions by the parties

It is FEU's position that "[t]he Commission, interveners and customers can rest assured that the FEU's information systems are appropriately configured, and the FEU have policies and procedures in place to protect personal information. This is an ongoing business requirement that the FEU manage today, regardless of where the data is stored."[71] FEU do not consider there to be incremental risk to storing data outside of Canada when the necessary risk, privacy and security assessments are completed.[72]

---

[66] FEU's privacy policy is shared with FortisBC Inc. and is thus FortisBC Utilities' (FBCU) privacy policy.
[67] Exhibit B-1, pp. 3–4.
[68] Exhibit B-3, BCUC IR 1.4.4.
[69] Exhibit B-6, CEC IR 1.7.1.
[70] Exhibit B-3, BCUC IR 1.4.2.
[71] Exhibit B-11, Alternative Relief BCSEA IR 1.8.13.
[72] Exhibit B-9, Alternative Relief BCUC IR 1.4.1.

CEC was the only intervener that specifically assessed FEU's security provisions. They submit that they have reviewed FEU's encryption and de-identification methodologies and FEU's general security provisions for assessing privacy requirements, establishing the boundaries of personal information and selecting vendors and have found that they are all sufficient.[73] Specifically CEC reviewed the information provided on the effectiveness and appropriateness of the encryption and de-identification methodologies and are satisfied that these processes will protect information.[74] Regarding unauthorized access CEC submits that the issue does not impact the application because the data is as accessible to hackers in a foreign jurisdiction as it would be in Canada.[75]

BCOAPO on the other hand, states that "FEU has not been able to store data outside of Canada. Its systems are designed in the context of a company that stores its data in Canada… How could the adequacy of the encryption and de-identification methods be assessed without an understanding of the specific contexts of the jurisdiction?"[76] BCOAPO submits that FEU lacked consultation with third party security experts in preparing the application and in particular the evidence on the updated proposal, including the risk of storing data in other jurisdictions and what types of protections would be required.[77]

FEU disagree with BCOAPO's position and submit that their assertion that data stored in a foreign jurisdiction is not subject to greater risk is based on expert evidence by FEU's Director of Information Systems and evidence that the FEU use third parties to validate this conclusion.[78]

5.3.7 Submissions on foreign government accessing FEU data in its own jurisdiction

FEU submit that the risk of foreign government access "is appropriately mitigated… because any customer, sensitive or FEU employee information obtained by a foreign government within its own jurisdiction will be encrypted or de-identified, and the encryption or de-identification keys will at all times be kept by the FEU within Canada. In other words, whatever data a foreign government obtains within its own jurisdiction will be useless information and not put the FEU or its customers at risk."[79]

BCSEA accepts that if a foreign government does not possess the keys the risk of disclosure of protected information may be small but that "access to the keys is the Achilles Heel" of the updated proposal.[80]
CEC submits that access by authorized foreign governments is one of the most significant risks associated with storing data outside Canada but that risk is mitigated by the de-identification and encryption keys being held in Canada.[81]

---

[73] CEC July 27, 2015 Final Submission, pp. 5–6.
[74] Ibid., p. 6.
[75] Ibid., p. 9.
[76] BCOAPO July 27, 2015 Final Submission, p. 7.
[77] Ibid.
[78] FEU August 4, 2015 Reply Submission, pp. 9–10.
[79] FEU June 30, 2015 Final Submission, p. 6.
[80] BCSEA July 27, 2015 Final Submission, pp. 3–4.
[81] CEC July 27, 2015 Final Submission, p. 8.

5.3.8 Submissions on foreign government ordering FEU to provide an encryption key across the Canadian border

FEU submit that there is no risk of a foreign government ordering FEU to provide encryption or de-identification keys because FEU is a Canadian owned and controlled company.

> Under the principles of international law, a foreign court cannot simply reach across the Canadian border to order the FEU to provide an encryption key… This risk only arises where the Canadian entity holding the encryption key is subject to control by a foreign corporate entity. The control may arise through a parent-subsidiary relationship…[82]

FEU further submit:

> [A] U.S. court will not have jurisdiction to issue an order compelling a Canadian company to perform or not to perform certain acts in a legal action that arises in Canada… FEU have not seen any case law or suggestions from the Office of the Information and Privacy Commissioner that this has been or will be the case.[83]

BCSEA disagree with this assessment and state:

- The FEU cite no principle(s) of international law, whether public international law or private international law, that categorically precludes a foreign court from making an order that has effect on a legal person within Canada. Canadian courts routinely give effect to foreign orders so as to cause legal effects on persons and property within Canada, subject to a large body of jurisprudence.
- The FEU argues that 'This risk only arises where the Canadian entity holding the encryption key is subject to control by a U.S. corporate entity.' With respect, that argument is patently incorrect. It would be naive to assume that the FEU are invulnerable to legally authorized foreign government action aimed at decrypting or re-identifying data seized within the foreign jurisdiction.
- Not only does the FEU's corporate parent have substantial assets located within the United States, even more importantly the FEU itself would have mission-critical assets within the foreign jurisdiction in the form of the encrypted or de-identified data. Presumably, a foreign entity intent on de-crypting or re-identifying the seized data would require the FEU to provide the keys as a prerequisite for the FEU being allowed access to its own data. How long would the FEU be able and willing to resist providing the keys in order to regain access to its crucial corporate information?

[82] Transcript Volume 2, p. 57; FEU June 30, 2015 Final Submission, pp. 6–7.
[83] Exhibit B-11, Alternative Relief BCSEA IR 1.17.4.4.

- The FEU have provided no evidence that an information service provider offers a service that includes even a contractual commitment that there would be no authorized foreign government access to encrypted or de-identified data from Canada that is stored in the foreign jurisdiction with the keys located within Canada.[84]

In reply, FEU submit that BCSEA provides no legal authority to support its assertions. FEU further state that "there is no *control relationship* between any foreign entity and the FEU that would create the risk that a foreign court might be able to obtain, through a foreign entity, an encryption key." With respect to BCSEA's submission that a foreign entity may not allow FEU to regain access to seized data unless the encryption/re-identification keys are provided, FEU state that "if a foreign court tried to extort a key… FEU would not comply" and "FEU would not put critical data into any situation where this kind of risk could occur."[85]

Based on the comments made by the BC Privacy Commissioner and FEU being Canadian owned and controlled, CEC accepts that "the risk of access by foreign governments is not of concern unless the ownership structure of the Company changes. The CEC recommends that the Commission incorporate a condition such that the removal of the data relocation restriction is subject to the FEU remaining a Canadian owned and controlled corporation."[86]

5.4 Panel discussion and determination

The task for this Panel is to identify whether security or privacy risks of storing data are increased by storing data outside Canada, and if so to what extent. The potential risks must then be weighed against potential benefits to determine if approving the application is in the public interest.

Regarding the risk of unauthorized access, the Panel accepts FEU's characterization that the digital universe has no borders and that if a person wants to "gain unauthorized access to data, that person could be located anywhere in the world, and the location of the data itself would not change that fact." As well, unauthorized access can occur from within the company through unauthorized employee or insider access. In the Panel's view, the risk of unauthorized access is not related to location of the data. Rather, the risk of unauthorized access is related to how comprehensive a company's data security and privacy regimes are.

The Panel finds that FEU have an adequate security and privacy protection regime for its data based on the FEU's:

- Use of current encryption and de-identification technology that will adequately protect data without the keys because of the computing power and time required to break the encryption or de-identification. The data if accessed would therefore be unreadable;
- Management of employee and contractor access to encryption and de-identification keys through access of least privilege protocols;

[84] BCSEA July 27, 2015 Final Submission, p. 4.
[85] FEU August 4, 2015 Reply Submission, pp. 3–4.
[86] CEC July 27, 2015 Final Submission, p. 8.

- Use of a comprehensive vendor selection process and strict vendor security and privacy requirements;
- Use of adequate security and privacy assessment process and criteria; and
- Regular audit and testing of their security measures by independent third parties.

The Panel further acknowledges that the relevant statues (PIPA and PIPEDA) legally require FEU to employ a comprehensive privacy protection regime.

The Panel has assessed BCOAPO's concerns that FEU's security and privacy protection measures have been developed in Canada and may not be adequate outside of Canada. The Panel notes that under FEU's updated proposal, the encryption and de-identification keys would be kept on FEU's servers in Canada. As noted above, the Panel finds that encryption and de-identification provide a high degree of protection, thus, if FEU's security or privacy measures were to fail outside of Canada, encrypted or de-identified data would be adequately protected.

Regarding privacy protection under PIPA and PIPEDA, FEU are legally responsible for the personal information under its control, including personal information that is not in its custody or that has been transferred to a third party. Thus, although those statutes do not dictate a privacy regime that must be used outside Canada, they do dictate that FEU must protect against all feasible threats because FEU are responsible and accountable for the privacy protection of the data.

In the Panel's view, FEU's security and privacy regime is adequate to mitigate the risk of unauthorized access. Regarding the risk of authorized foreign government access, all parties agree that locating data outside of Canada does present this risk because data is subject to the laws of the jurisdiction in which it is stored.

Therefore, the question for the Panel is whether FEU's mitigation strategies are adequate to protect against this risk. FEU's primary mitigation strategy is encrypting and de-identifying certain data while keeping the encryption and de-identification keys in Canada. FEU assert that while a foreign government may compel the provision of data held within its jurisdiction, they cannot compel the provision of the encryption or de-identification keys that are necessary to make the data readable or useful. The question of whether a foreign government can compel the keys became a subject of legal submissions in this proceeding.

As noted above, the Panel agrees that encryption and de-identification is so difficult to break without the keys that the relevant consideration for this risk assessment is whether a foreign government can compel the provision of keys stored by FEU in Canada through the foreign judicial system.

The Panel is persuaded by FEU's assessment that under the principles of international law a foreign authority may not legally compel FEU, which are owned and controlled by a Canadian company, to provide encryption and/or de-identification keys, unless ordered to do so by the Canadian court. In the Panel's view a Canadian court proceeding offers protection for the keys because it would likely consider customer interests of the

Canadian company in its decision. The key factor of this protection, however, is that FEU are Canadian owned and controlled by their parent company, Fortis Inc. which is located in Canada. Therefore, the Panel agrees with CEC's submission that a condition should be in place such that if this Panel grants the removal of the data relocation restriction it should be subject to FEU remaining a Canadian owned and controlled company.

6.0 OTHER MATTERS

6.1 Definitions of data to be encrypted or de-identified

The updated proposal includes specific definitions of customer, employee and sensitive data that would be subject to encryption and de-identification. At the close of evidence in this proceeding these definitions were not finalized, and it was agreed that FEU and the interveners would discuss the definitions and based on these discussions FEU would suggest definitions in their final submission.[87] The definitions proposed are:

- "**Customer Information**" means information of or about the FEI residential, commercial, or industrial customers.
- "**Employee Information**" means information of or about the FEI employees.
- "**Sensitive Information**" includes:
  - financial, commercial, scientific or technical information, the disclosure of which could result in undue financial harm or prejudice to the FEI; and
  - information that relates to the security of the FEI critical infrastructure and operations, the disclosure of which could pose a potential threat to the FEI operations or create or increase the risk of a debilitating impact on the safe and reliable operation of the FEI system.

Regarding the definitions proposed by FEU in the updated proposal, CEC submits that "the scope of information subject to de-identification and/or encryption is sufficiently broad to encompass all the necessary information and recommends that the Commission approve the above definitions."[88]

BCSEA provided comment on the term "personal information" in so far as they submit that FEU's confirmation in their final submission that the definition of personal information would be applied to all customers has clarified this definition and resolved BCSEA's concern.[89]

Concerns were raised in the proceeding about the level of oversight and monitoring FEU will have of the determination of what is sensitive data. FEU state that it will:

> necessarily involve some professional judgment, just like we employ professional judgment on all of our decision making… Because whether or not this restriction exists, we deal with sensitive data on a regular basis and have to protect it within our system, not just if we take it out of our systems. So it is just part of our normal business. It's not something over and above.[90]

---

[87] Transcript Volume 2, pp. 201–203.
[88] CEC July 27, 2015 Final Submission, p. 4.
[89] BCSEA July 27, 2015 Final Submission, p. 3, Footnote 11.
[90] Transcript Volume 2, pp. 197–199.

BCOAPO raises concerns that the decisions about whether information is considered "customer" or "sensitive" would be left solely to FEU if the updated proposal is approved. "In BCOAPO's view there was a lack of emphasis on oversight and monitoring of the decisions relating to the compliance with the proposed order in the Application. FEU has not stored data outside of Canada before –this would be a new model and the proposed order has a number of modifiers that require monitoring."[91]

6.2 Suggested wording changes by CEC on the updated proposal

In its final submission, CEC recommends that the Commission approve the requested order with three modifications to the wording.[92] The following briefly describes CEC's recommended changes:

(1) In section (c), change "stored on servers located outside Canada" to "transmitted to other parties or stored in locations outside of Canada."

(2) In section (b) related to the definitions of "Encrypted" and "De-identified", change "current" to "best industry standards" for encryption and "best industry practice" for de-identification.

(3) In section (d), change "stored on servers" to "stored and managed using secure methodologies, in secure FEU facilities, meeting best in industry standards, located in Canada and as approved by the BC Utilities Commission."

In their reply submission, FEU explain why each of CEC's recommended wording modifications should not be adopted. With respect to (1), FEU explain that the current data restriction is about storage of data, and not its transmittal. The order should only be concerned with storage on servers located outside of Canada.[93] With respect to (2), FEU submit that a "best practices" standard is too subjective and unclear. Another concern is that "best practice" may change in short spans of time and FEU would be required to switch technology more often than truly necessary in order to ensure that the "best practice" standards are met, which may be expensive.[94] With respect to (3), FEU submit that the meaning of "stored and managed using secure methodologies, in secure FEU facilities" is unclear and not necessary, as data centres are protected by a robust security network.[95]

6.3 Reporting requirements

BCSEA submits that the Commission should add a reporting requirement if the Commission approves FEU's updated proposal. BCSEA suggests that the annual Performance Based Ratemaking review would be an appropriate and efficient place for such reporting. The reporting should address information security measures as well as the costs and savings associated with storing information outside of Canada.[96]

BCOAPO states that FEU have not stored data outside of Canada before and the proposed order has a number of modifiers that require monitoring.[97]

---

[91] BCOAPO July 27, 2015 Final Submission, pp. 7–8.
[92] CEC July 27, 2015 Final Submission, pp. 5–7.
[93] FEU August 4, 2015 Reply Submission, p. 11.
[94] Ibid., p. 12.
[95] Ibid., pp. 13–14.
[96] BCSEA July 27, 2015 Final Submission, p. 5.
[97] BCOAPO July 27, 2015 Final Submission, p. 8.

FEU submit that there should not be any further reporting requirements or restrictions put in place as FEU do not believe that risk increases as a result of where the data is stored and there is no particular oversight monitoring needed of what is essentially a matter of the "day-to-day management of the utility."[98]

If reporting is necessary, FEU submit that FEU could provide the Commission with an Internal Audit report which would be subject to an audit protocol to ensure the factual accuracy of observations. The report would be negative assurance reporting that confirms that the FEU are complying with the order granted in this proceeding.[99]

7.0 FINAL SUBMISSIONS

Both BCOAPO and BCSEA oppose FEU's Application and updated proposal.

BCOAPO requests that the Commission reject FEU's application because the application has flawed and underdeveloped rationales and highlights the privacy and security risks of customer information. BCOAPO concludes that "an application to remove the Data Restriction entirely may be better placed in the context of an application seeking the Commission's approval of a specific proposal for data storage in a foreign jurisdiction."[100]

BCSEA states that FEU have not proven that the updated proposal would be in the public interest because they maintain a primary concern about authorized foreign government access.[101] BCSEA submits that the Commission should maintain the status quo under which the FEU are at liberty to apply to the Commission for approval of a specific project.[102]

CEC concludes that the Commission should approve the requested order sought with CEC's proposed wording modifications because data stored outside of Canada would be as secure and private as data stored in Canada, except for the potential for foreign governments to lawfully access or permit access to data stored in their country which is not of concern unless ownership structure of the company changes.[103]

FEU submit that it is inefficient and impractical to apply for specific exemptions each time it wishes to engage a third party data service outside of Canada. The updated proposal will allow FEU to access a range of service providers who can provide benefits, both small and large. FEU conclude that the data restriction should be removed, and the updated proposal should be granted, so that the FEU can pursue technology solutions that will benefit customers.[104]

---

[98] Transcript Volume 2, p. 192.
[99] FEU August 4, 2015 Reply Submission, p. 5.
[100] BCOAPO July 27, 2015 Final Submission, p. 8.
[101] BCSEA July 27, 2015 Final Submission, p. 3.
[102] Ibid., p. 4.
[103] CEC July 27, 2015 Final Submission, pp. 2, 8, 10; CEC December 11, 2014 Final Submission, p. 2.
[104] FEU June 30, 2015 Final Submission, p. 14; FEU August 4, 2015 Reply, p. 14.

7.1 Panel discussion and determination

As determined previously, there are potential benefits available if the restriction is lifted and the pursuit of cost savings is consistent with the Performance Ratemaking Plan which FEU are currently under. Thus, it is the Panel's view that FEU should be given the opportunity to pursue these potential benefits for themselves and their customers *if* the risk to the company and its customers do not outweigh the potential benefits.

As noted above, there are risks to storing data anywhere, but FEU have adequately mitigated these risks through its security and privacy protection regimes. The incremental risk to storing data outside of Canada is the risk of lawful foreign government access but, as found above, the updated proposal protects against this risk by encrypting/de-identifying data and maintaining the keys within Canada as long as FEU remain Canadian controlled and owned.

Given that the risks are sufficiently mitigated, the Panel considers that it is in the public interest for FEU to be given the opportunity to pursue the potential benefits. **Therefore, the Panel approves the updated proposal subject to FEI continuing to be owned and controlled by a Canadian company located in Canada.**

Regarding the definitions of customer, employee and sensitive data included in the updated proposal, the Panel notes no intervener raised objection to these definitions. The Panel finds these definitions are adequately broad to ensure the necessary data is protected. The Panel is not concerned about the fact that FEU would determine what data fits into these three categories because the Panel accepts FEU's evidence that they have to protect data as part of their normal business. In the Panel's view, FEU have a great deal to lose in terms of reputation and costs if their data is not adequately protected and thus they have an interest in effectuating these definitions in a broad manner.

The Panel has considered the submissions from BCOAPO and BCESA regarding reporting requirements and finds that some level of reporting is warranted so the Commission and participants in this proceeding can monitor outcomes, if any, of this decision.

With respect to data and servers located outside of Canada, FEI is to provide the Commission with a report prepared by its Internal Audit group detailing:

- **any significant security and/or privacy breaches and the resolution process; and**
- **any significant deficiencies identified in processes and controls and the remediation process.**

FEI is directed to file this report on an annual basis. FEI is to submit the date that is most practical for the company to file this report annually to the Commission by no later than November 30, 2015.

The Panel is not persuaded that the report should be reviewed in the annual Performance Based Ratemaking review process. The reporting will allow the Commission and participants in this proceeding to monitor whether FEI is employing and adhering to their identified risk mitigation strategies. Any cost savings associated with storing information outside of Canada will be recognized in the overall operations and maintenance costs included in the Performance Based Ratemaking Annual Review.

The Panel has considered CEC's suggested wording changes but is satisfied with the wording in the FEU updated proposal. **The Panel approves the updated proposal with the terms set out in section 1.2 of this decision.** However, while the Panel accepts FEU's proposed wording that "best" industry standards/practices may be too subjective, the Panel has concerns with FEU's explanation that "best" standards/practices would lead to more frequent updates and costs as compared to "current" standards/practices.

The Panel notes that it would not be prudent of FEU to fail to appropriately update its standards or practices as knowledge and technologies evolve. This is equally true for protecting data stored within Canada as well as any data stored in a foreign jurisdiction. The Panel expects FEU to update their standards and practices as often as needed to ensure that customer, employee and sensitive information is properly secured.

DATED at the City of Vancouver, in the Province of British Columbia, this 13th day of October 2015.

Original signed by:

L. A. O'HARA
PANEL CHAIR / COMMISSIONER

Original signed by:

N. E. MACMURCHY
COMMISSIONER

Original signed by:

K. A. KEILTY
COMMISSIONER

SIXTH FLOOR, 900 HOWE STREET, BOX 250
VANCOUVER, BC V6Z 2N3 CANADA
web site: http://www.bcuc.com

BRITISH COLUMBIA UTILITIES COMMISSION

ORDER NUMBER G-161-15

TELEPHONE: (604) 660-4700
BC TOLL FREE: 1-800-663-1385
FACSIMILE: (604) 660-1102

IN THE MATTER OF
the Utilities Commission Act, R.S.B.C. 1996, Chapter 473

and

An Application by the FortisBC Energy Utilities consisting of FortisBC Energy Inc., FortisBC Energy (Vancouver Island) Inc. and FortisBC Energy (Whistler) Inc. for Removal of the Restriction on the Location of Data and Servers Providing Service to the FEU currently Restricted to Canada

BEFORE: L. A. O'Hara, Panel Chair/Commissioner
N. E. MacMurchy, Commissioner
K. A. Keilty, Commissioner

October 13, 2015

O R D E R

WHEREAS:

A. On August 1, 2014, the FortisBC Energy Utilities (FEU) applied to the British Columbia Utilities Commission (Commission) for removal of the restriction on the location of data and servers providing service to the FEU, currently restricted to Canada (Application). The current restriction was established by Orders G-116-05, G-75-06, and G-49-07, and clarified by Letter L-30-06 and states:

> *[T]he Commission orders that the location of data and servers providing service to the [FEU] is to be restricted to Canada and that any proposal to locate data and servers providing services to the [FEU] (including data and servers providing back-up services) outside Canada will require the Commission's approval.*

B. By Orders G-126-14, G-150-14, G-184-14 and G-26-15, and letter dated June 15, 2015, the Commission established the public hearing process and the regulatory timetable for the Application;

C. While FEU were the original applicant in this proceeding, the companies that comprised FEU were amalgamated on December 31, 2014, and the amalgamated entity carries on business under the name FortisBC Energy Inc. (FEI). FEI is Canadian owned and controlled by their parent company, Fortis Inc., which is located in Canada;

.../2

D. The approval sought by FEI is as follows:

(e) Effective the date of this order, the restriction imposed under Orders G-116-05, G-75-06, and G-49-07, that the location of data and servers providing service to FEI be restricted to Canada, is removed and no longer in effect.

(f) For the purposes of this order:

- "**Customer Information**" means information of or about the FEI residential, commercial, or industrial customers.
- "**Employee Information**" means information of or about the FEI employees.
- "**Sensitive Information**" includes:
  - financial, commercial, scientific or technical information, the disclosure of which could result in undue financial harm or prejudice to the FEI; and
  - information that relates to the security of the FEI critical infrastructure and operations, the disclosure of which could pose a potential threat to the FEI operations or create or increase the risk of a debilitating impact on the safe and reliable operation of the FEI system.
- "**Encrypted**" means an encryption methodology using current industry standards for secure encryption.
- "**De-identified**" means a de-identification methodology consistent with current industry practice for the purpose of protecting personal information.
- "**Encryption keys**" and "**De-identification keys**" mean any information or methodology used to access encrypted or de-identified data.

(g) Effective as the date of this Order, FEI is permitted to store data on servers located outside of Canada, provided that data containing **Customer Information, Employee Information,** or **Sensitive Information,** or any combination thereof, must be either **Encrypted** or **De-identified** if such data is to be stored on servers located outside of Canada.

(h) **Encryption keys** and **De-identification keys** for **Encrypted** or **De-identified** FEI data stored outside of Canada must be stored on servers located within FEI's data centres that are located in Canada.

E. Three interveners registered for the proceeding: (i) the Commercial Energy Consumers Association of British Columbia (CEC), (ii) British Columbia Sustainable Energy Association and the Sierra Club of British Columbia (BCSEA), and (iii) British Columbia Old Age Pensioners' Organization *et al.* (BCOAPO);

F. Section 44 of the *Utilities Commission Act* is the only section of the statute that addresses the location of public utility records and states:

(1) A public utility must have in British Columbia an office in which it must keep all accounts and records required by the commission to be kept in British Columbia.

(2) A public utility must not remove or permit to be removed from British Columbia an account or record required to be kept under subsection (1), except on conditions specified by the Commission. The Panel reviewed and considered all evidence on record for the application and determines that the approved sought as contained in Recital D, is in the public interest and should be approved subject to certain conditions.

NOW THEREFORE pursuant to section 44 of the *Utilities Commission Act*, for the reasons set out in the decision that is issued concurrently with this order, the Commission approves FortisBC Energy Inc.'s application as set out in Recital D of this order subject to FortisBC Energy Inc. continuing to be owned and controlled by a Canadian company located in Canada. FortisBC Energy Inc. is to comply with all determinations and directives set out in the decision.

DATED at the City of Vancouver, in the Province of British Columbia, this 13th day of October 2015.

BY ORDER

Original signed by:

L. A. O'Hara
Panel Chair / Commissioner

IN THE MATTER OF
the Utilities Commission Act, R.S.B.C. 1996, Chapter 473

and

FortisBC Energy Utilities

Application for Removal of the Restriction on the Location of Data and Servers Providing Service to the FEU, currently Restricted to Canada

EXHIBIT LIST

Exhibit No.	Description
COMMISSION DOCUMENTS	
A-1	Letter Dated August 26, 2014 - Appointment of Panel
A-2	Letter dated August 29, 2014 – Order G-126-14 Establishing a Regulatory Timetable
A-3	Letter dated September 24, 2014 – Order G-150-14 Issuing an Amended Regulatory Timetable
A-4	Letter dated September 29, 2014 – Commission Response to FEU Request for Extension to file IR No. 1 Responses
A-5	Letter dated October 14, 2014 – Commission Information Request No. 1 to FEU
A-6	Letter dated November 18, 2014 – Commission proposal for Final Submission Phase
A-7	Letter dated November 26, 2014 – Final Submission Phase
A-8	Letter dated December 30, 2014 - Request for Submissions regarding the Alternative Relief
A-9	Letter dated January 20, 2015 – Procedural Conference on Alternative Relief
A-10	Letter dated January 30, 2015 – Notice of member extension
A-11	Letter dated February 24, 2015 – Order G-26-15 with reasons, Establishing a Regulatory Timetable
A-12	Letter dated April 7, 2015 – Commission Information Request No. 1 on Alternative Relief to FEU
A-13	Letter dated May 26, 2015 – Commission Panel notice regarding the Streamlined Review Process
A-14	Letter dated June 15, 2015 – Regulatory Timetable

A2-1 Letter dated June 11, 2015 – Staff submission "Microsoft Cloud Touches Down in Canada" - Microsoft Canada; and "Microsoft to build two data centres in Canada as it expands cloud services" - The Globe and Mail

APPLICANT DOCUMENTS

B-1 **FORTISBC ENERGY UTILITIES (FEU)** Letter Dated August 1, 2014 - Application for Removal of the Restriction on the Location of Data and Servers Providing Service to the FEU, currently Restricted to Canada

B-2 Letter dated September 25, 2014 – FEU Submitting Extension Request

B-3 Letter dated November 12, 2014 - FEU Response to BCUC IR No. 1

B-4 Letter dated November 12, 2014 - FEU Response to BCOAPO IR No. 1

B-5 Letter dated November 12, 2014 - FEU Response to BCSEA IR No. 1

B-6 Letter dated November 12, 2014 - FEU Response to CEC IR No. 1

B-7 Letter Dated December 24, 2014 - FEU Response to BCSEA Request for Sur Reply Submission (Exhibit C2-3)

B-8 Letter Dated March 17, 2015 - FEU Submitting Evidence on Alternative Relief

B-9 Letter Dated April 23, 2015 - FEU Response to BCUC IR No. 1 on Alternative Relief

B-10 Letter Dated April 23, 2015 - FEU Response to BCOAPO IR No. 1 on Alternative Relief

B-11 Letter Dated April 23, 2015 - FEU Response to BCSEA IR No. 1 on Alternative Relief

B-12 Letter Dated April 23, 2015 - FEU Response to CEC IR No. 1 on Alternative Relief

B-13 Letter Dated June 12, 2015 - FEU Submitting SRP Presentation

INTERVENER DOCUMENTS

C1-1 **COMMERCIAL ENERGY CONSUMERS ASSOCIATION OF BRITISH COLUMBIA (CEC)** Letter Dated September 12, 2014 – Request for Intervener Status by Christopher Weafer

C1-2 Letter Dated October 21, 2014 - CEC Submitting Information Request No. 1 to FEU

C1-3 Moved to Arguments

C1-4 Letter dated April 7, 2015 – CEC IR No. 1 on Alternative Relief to FEU

C1-5 Letter dated April 27, 2015 – CEC will not be submitting Intervener Evidence on Alternative Relief

C2-1 **BC SUSTAINABLE ENERGY ASSOCIATION AND THE SIERRA CLUB OF BRITISH COLUMBIA (BCSEA)** Letter Dated September 29, 2014 – Request for Intervener Status by William J. Andrews and Thomas Hackney

C2-2 Letter Dated October 20, 2014 - BCSEA Submitting Information Request No. 1 to FEU

C2-3 Letter Dated December 23, 2014 - BCSEA Request for Sur Reply Submission

C2-4 Moved to Arguments

C2-5 Letter dated April 7, 2015 – BCSEA Information Request on Alternative Relief to FEU

C2-6 Letter dated April 27, 2015 – BCSEA Submitting Comments regarding Filing of Evidence

C3-1 **BRITISH COLUMBIA PENSIONERS' AND SENIORS' ORGANIZATION (BCPSO ET AL)** Letter Dated October 14, 2014– Request for Intervener Status by Tannis Braithwaite, Lobat Sadrehashemi and James Wightman

C3-2 Letter Dated October 21, 2014 - BCOAPO Submitting Information Request No. 1 to FEU

C3-3 Moved to Arguments

C3-4 Letter dated April 7, 2015 – BCOAPO IR No. 1 on Alternative Relief to FEU

INTERESTED PARTY DOCUMENTS

D-1 **COOKE, BILL (COOKE)** Letter Dated September 19, 2014 – Request for Interested Party Status