Fasken Martineau DuMoulin LLP *
Barristers and Solicitors
Patent and Trade-mark Agents

2900 – 550 Burrard Street
Vancouver, British Columbia, Canada V6C 0A3

604 631 3131 Telephone
604 631 3232 Facsimile
1 866 635 3131 Toll free

www.fasken.com

FASKEN MARTINEAU

David Curtis
Direct +1 604 631 4827
Facsimile +1 604 632 4827
dcurtis@fasken.com

June 30, 2015
File No.: 240148.00740/15951

BY ELECTRONIC FILING

British Columbia Utilities Commission
Sixth Floor, 900 Howe Street
Vancouver, BC V6Z 2N3

Dear Sirs/Mesdames

Re: FortisBC Energy Utilities (FEU) - Remove Data Location Restriction

In accordance with the Commission's letter of June 15, 2015 (Ex. A-14) in this proceeding, we enclose for filing the electronic version of the FEU's final submissions.

Hardcopies of the enclosed will follow by courier.

Yours truly,

FASKEN MARTINEAU DuMOULIN LLP

[Original signed by David Curtis]

David Curtis

/DC

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

Submissions of FortisBC Energy Utilities
following June 12, 2015, SRP

June 30, 2015

TABLE OF CONTENTS

A. INTRODUCTION 1

B. ISSUES RAISED DURING THE SRP 2

(a) Updated Alternative Relief 2

(b) Access to Data by a Third Party 5

(c) The Microsoft Canada Project 10

(d) Segregating FEU and FBC data 11

(e) Commission Staff Questions Regarding Controls 11

C. GOING FORWARD 12

D. BENEFITS 13

E. CONCLUSION 14

A. INTRODUCTION

1. In Orders G-116-05, G-75-06, and G-49-07, and Letter L-30-06, the Commission established a restriction that requires the FortisBC Energy Utilities (FEU)[1] to store all of their data on servers located within Canada (the Data Restriction). On August 1, 2014, the FEU applied to the Commission for an order removing the Data Restriction (Exhibit B-1, the Application).

2. The Application was concluded with a hearing in the format of a Streamlined Review Process (SRP) so that interveners, Commission staff and the Commission Panel could engage in direct dialogue with the FEU's subject-matter experts regarding matters raised in the Application. The SRP process was a helpful, constructive and engaging forum to address issues of concern raised by those who attended. The FEU's primary submissions following the SRP are that:

(a) the updated alternative relief discussed in this final submission addresses a number of key intervener concerns raised at the SRP;

(b) the remaining issues of concern discussed during the SRP are appropriately addressed by the FEU; and

(c) as a result, the Data Restriction should be rescinded and the alternative relief (as updated following the SRP) should be granted.

3. These submissions are focussed on issues of concern raised during the SRP, and are not intended to canvass all of the issues raised in this proceeding to date. The FEU continue to rely on the detailed written arguments in both final and reply submissions previously filed in this proceeding.

4. The following topics are addressed below:

---

[1] Previously comprised of FortisBC Energy Inc., FortisBC Energy (Vancouver Island) Inc., and FortisBC Energy (Whistler) Inc., and now FortisBC Energy Inc. as a result of amalgamation.

(a) the updated alternative relief, which addresses issues raised during the SRP regarding the protection of corporate customer information, "sensitive" information, and FEU employee information;

(b) access to data by a third party;

(c) the Microsoft Canada project;

(d) segregating FEU and FBC data;

(e) Commission staff questions;

(f) the FEU's approach going forward if the alternative relief is granted; and

(g) the potential for customer benefits.

5. For the reasons set out below, the FEU submit that the updated alternative relief sought should be granted.

B. ISSUES RAISED DURING THE SRP

(a) Updated Alternative Relief

6. During the SRP, interveners raised concerns regarding three key categories of data, and the manner in which they were addressed under the initial draft of the alternative relief sought.

Corporate Customer Information

7. One of the issues raised during the SRP was a concern that data about corporate customers was not expressly addressed in the initial version of the alternative relief.[2] In response to this concern, the FEU confirmed that from a data protection perspective, it treats corporate customer information in the same way that it treats personal (or "individual") customer information.[3] The FEU confirmed that it was willing to revise the draft order sought so that the order confirms that corporate customer information would be protected.[4] The

---

[2] Transcript - Volume 2, p. 79, starting at line 17.

[3] Transcript - Volume 2, p. 79, lines 9-16.

[4] Transcript - Volume 2, p. 82, lines 12-21.

updated alternative relief now incorporates this commitment. The updated alternative relief is set out below.

8. The FEU submits that it has addressed the concerns raised regarding the treatment of corporate customer information.

Sensitive Information

9. During the SRP Interveners raised concerns about access to non-customer, but "sensitive" information concerning, for example, the utility's operations.[5] In response to this concern, the FEU confirmed that any data that the FEU believe is sensitive will be encrypted or de-identified before leaving the FEU's network.[6] The FEU have modified the alternative relief sought to make this commitment an express provision of the order, which is set out below.

10. FEU submits that it has addressed the concerns raised regarding the treatment of sensitive utility information.

FEU Employee Information

11. During the SRP Commission staff asked whether FEU employee information would be encrypted or de-identified if the order is granted, and the FEU confirmed that it would be.[7] The modified alternative relief sought addresses this commitment as well.

Encryption and De-identification Keys

12. Given the concerns with foreign government and unauthorized access discussed at the SRP, it may be appropriate to make it an express term of the modified alternative relief that encryption and de-identification keys must, at all times, be kept within Canada and within the FEU's network. This modification is set out below.

---

[5] See for example, Transcript - Volume 2, p. 83, line 15 to p. 84, line 2; p. 90, lines 9 to 19.

[6] Transcript - Volume 2, p. 90, lines 20-24.

[7] Transcript - Volume 2, p. 185, lines 17-25.

The Modified Alternative Relief

13. As a result of the feedback describe above, the FEU revised the alternative relief and circulated a draft form of order to interveners for comment prior to filing this submission. Comments were received back from each of CEC, BCOAPO and BCSEA. Whether the comments were provided without prejudice or not, out of an abundance of caution the FEU are not discussing any of the feedback received in this submission, other than to say that the FEU have considered the feedback and incorporated some of the suggested edits.

14. Accordingly, the FEU are now seeking the following modified alternative relief:

(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 the 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's residential, commercial, or industrial customers.
- **"Employee Information"** means information of or about the FEI's 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's critical infrastructure and operations, the disclosure of which could pose a potential threat to the FEI's operations or create or increase the risk of a debilitating impact on the safe and reliable operation of the FEI's 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.

15. The different wording in the definitions for "encrypted" and "de-identified" reflects the fact that while encryption has recognized industry "standards", de-identification usually speaks to an industry practice based on legislation or regulatory guidelines or policies.

(b) Access to Data by a Third Party

16. The topic of the risk of access to FEU data by a foreign government pursuant to lawful authority, or an unauthorized third party (i.e. by hacking), was raised by all three interveners in attendance at the SRP, by Commission staff and by the Panel. The following exchange summarizes the FEU's position regarding both issues:

> COMMISSIONER MACMURCHY: Just to make sure we're absolutely clear then. Really what you're saying is from the unauthorized side [the risk to customers] doesn't change because the digital world is the digital world and it doesn't have boundaries. From the authorized side what you're saying is that yes, they may be able to get the raw data but it'll be encrypted or detokenized form, and we'll hear the legal arguments about the ability to compel the keys. But normally the expectation would be that unless a Canadian court agrees, that those keys would not be accessible. Is that sort of --
>
> MR. D. SWANSON: Correct.[8]

17. The following submissions provide further detail on these matters.

---

[8] Transcript - Volume 2, p. 134, lines 13-24.

Authorized Foreign Government Access

18. If data is stored in a foreign jurisdiction, then that data is subject to foreign laws that could require the provision of the stored data to a foreign government. There are two aspects to this risk, both of which are appropriately addressed by the FEU.

19. 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. This risk is appropriately mitigated by the alternative relief 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.

20. The risk that a foreign government can decrypt encrypted FEU data is extraordinarily low. As the FEU have described, the encryption standard that is used by the FEU is "considered fundamentally impossible to decrypt… There simply not enough processing power on the planet to brute-force decrypt the data that has been encrypted using FortisBC's methodologies".[9] It is not reasonably possible to re-identify de-identified data because the data is removed completely or replaced with random information.[10]

21. The 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. As described below, this is not a risk in the case of the FEU because it is a Canadian owned and controlled company.

22. 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. The potential risk, if any, is as identified by the Privacy Commissioner for British Columbia in the following:

> As this Office's 2004 report on the topic demonstrated, personal information stored in Canada may be accessed by foreign governments <u>where a company</u>

[9] Transcript - Volume 2, p. 64, lines 8-17.

[10] Transcript - Volume 2, p. 64, lines 18-23.

> 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 crosswalk table itself.[11] [Emphasis added.]

23. What the Privacy Commissioner is describing in the above passage is a risk that arises when a U.S. corporation (for example), situated in the U.S., has a corporate relationship with a Canadian entity. The risk is that a U.S. court could exercise its territorial jurisdiction over the U.S. corporation, and require that U.S. corporation to exert its corporate powers over a Canadian subsidiary. In that specific scenario, you could potentially have a situation in which a Canadian entity holding an encryption key could be compelled to provide the key to a U.S. entity pursuant to the corporate relationship, and the U.S. entity in turn might be under a court order to provide the key to a foreign government.

24. This risk only arises where the Canadian entity holding the encryption key is subject to control by a U.S. corporate entity. The control may arise through a parent-subsidiary relationship, or in one of the other manners described by the Commissioner in her letter, such as:

- [where] there is an intermingling of directors, officers, or employees between the parent and the subsidiary;
- The ability of the parent to direct the appointment of the subsidiary's directors, either directly or indirectly through another corporation or series of corporations;
- The ability of the parent to control the directors of the subsidiary;
- Common ownership or the ability to otherwise exercise control over the subsidiary; and
- Whether the subsidiary is incorporation in the United States or has continuous and systematic contact with the United States.[12]

---

[11] Excerpted by the FEU in Ex. B-8, at p. 8. The full letter containing this statement is found in Ex. B-8, Appendix D.

[12] Excerpted by the FEU in Ex. B-8, at p. 8. The full letter containing this statement is found in Ex. B-8, Appendix D.

25. These examples demonstrate that the concern arises out of the existence of some form of a control relationship between a U.S. entity and a Canadian entity. That relationship of corporate control is what has the potential to reach across the border; it is not that U.S. or any other foreign courts can directly impose their jurisdiction on Canadian entities. When there is no such control relationship between foreign and Canadian entities, there is no such risk.

26. As the FEU have made clear in this proceeding, this risk does not arise for the FEU because FortisBC Energy Inc., the legal entity after amalgamation of the FEU, is a Canadian owned and controlled company. As Ms. Pratch described in the SRP process:

> The risk identified is simple. The question is whether a foreign court can compel disclosure of data held by a Canadian company that's located in Canada. There is no evidence to suggest that this is possible, but rather, FortisBC accepts the position and guidance that has been published by the British Columbia office of the Information and Privacy Commissioner. That guidance states that there is a privacy risk of an American court compelling disclosure records where the records are held by American companies or their foreign subsidiaries. FortisBC submits that the issue raised regarding jurisdiction of a foreign -- of foreign courts to compel disclosure of data held by a Canadian company is not a risk, given that the FEU are Canadian-owned and controlled.[13] [Emphasis added.]

Unauthorized Access

27. Another issue raised during the SRP was a concern about unauthorized access to FEU data stored in a foreign jurisdiction. The FEU submit that this issue does not impact the application because the storage of data outside of Canada does not increase the risk of unauthorized access.

28. During the SRP, Ms. Pratch summarized why the risk of unauthorized access does not increase when data is stored outside of Canada as follows:

> Now with respect to the concern over the risk of access to information. FortisBC submits that there is no greater risk that that information will be accessed by an

[13] Transcript - Volume 2, p. 55, line 18 to p. 56, line 7.

> unauthorized party by storing that information outside of Canada. And there are two main reasons that I'd like to provide to give support to this assertion.
>
> 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 data that is not -- sorry. In the unlikely event of a breach of that data, it wouldn't be protected by borders.
>
> The issue really comes down to the security that you put around that data. And FortisBC once again uses the same high level of security requirements regardless of where that data is stored. Whether we put that security around data stored in Canada, around data stored in the U.S., around data stored in England, or anywhere else in the world, that data and the requirements, the security requirements, are the same.
>
> Accordingly, the storage of data outside of Canada does not increase the risk of unauthorized access to that data.[14]

29. In short, it does not matter where data is located in terms of addressing unauthorized access risk; what matters is the security that a company places around the data wherever you store it. The FEU have stated throughout this proceeding that the security that will be put around any data stored in a foreign jurisdiction will be the same level of security that is placed around FEU data stored on Canadian soil. The FEU simply will not do business with any vendor who cannot meet the FEU's high security standards.[15] As Mr. Swanson stated during the SRP:

> Security risk assessments are a little bit more prescriptive. Our requirements are not negotiable, as I indicated in my presentation. It is a lot more black and white. And if we see any failures in that security assessment, the project will not go

[14] Transcript - Volume 2, p. 56, line 9 to p. 57, line 6.

[15] Transcript - Volume 2, p. 55, line 18 to p. 56, line 7.

> ahead unless the vendor is able to change their capabilities or their offering to meet our requirements.[16] [Emphasis added.]

30. For these reasons, the FEU submit that there is no increased risk of unauthorized access based on where data is stored. Furthermore, as with the foreign government access risk, even if a third party obtains FEU data stored outside of Canada, any customer, sensitive or FEU employee information unlawfully obtained by a third party will be encrypted or de-identified, and the encryption or de-identification keys will at all times be kept by the FEU within Canada. Accordingly, any data unlawfully obtained will be useless to the party receiving it.

(c) The Microsoft Canada Project

31. Prior to the SRP proceeding, Commission staff submitted Exhibit A2-1 which consisted of a press release from Microsoft and an article from the Globe and Mail regarding Microsoft's plan to deliver commercial cloud services from Canada, including products such as Azure and Office 365. As the FEU explained during the SRP, the Microsoft products described in Exhibit A2-1 are nothing more than examples of the kinds of services that the FEU are considering, and that there are a number of other potential services that the FEU would like to explore that are not offered in Canada.[17]

32. The FEU also explained that because the announced data centres will be located in Eastern Canada, there may be latency issues and even if the FEU wanted to use these Microsoft services, it still may have to use the U.S. data centres given that there are no announced plans for Microsoft to place data centres in Western Canada.[18]

33. The FEU submit that the Microsoft announcement has no impact on the application.

---

[16] Transcript - Volume 2, p. 148, line 23 to p. 149 line 4.

[17] Transcript - Volume 2, p. 93, line 5 to line 16.

[18] Transcript - Volume 2, p. 93, line 17 to p. 94, line 7.

(d) Segregating FEU and FBC data

34. During the SRP, the FEU confirmed that the FEU and FBC share platforms in order to provide efficiencies and achieve cost savings.[19] In light of this, an issue discussed during the SRP was whether lifting the Data Restriction might inadvertently cause the FEU to run afoul of provisions that were imposed on FBC in the AMI Decision.[20] The FEU confirmed that customer information is segregated between the electric and gas utilities, and that the distinction is clear and defined as between the two.[21]

(e) Commission Staff Questions Regarding Controls

35. During the SRP, Commission staff raised questions regarding the mechanics of the FEU's security assessments, privacy impact assessments, vendor due diligence and related matters. The FEU do not intend to review in any detail the various issues discussed, but wish to draw attention to a few of the key themes and issues discussed with Commission staff, all of which in the FEU's submission support granting the order sought:

(a) The FEU do not allow organizations who handle the FEU's data to have different processes in the handling of its data. If a vendor does not comply with the FEU's requirements in regard to processing and handling of data, the FEU do not use that vendor.[22]

(b) The FEU's security assessment process ensures that potential risks are addressed no matter where data is located.[23]

(c) The ultimate objective of privacy impact and security assessments is to ensure the safety of FEU's data, and to ensure that the level of safety will remain the same if a vendor is going to store data, as if the FEU were storing the data itself.[24]

---

[19] Transcript - Volume 2, p. 106, lines 14-26.

[20] Transcript - Volume 2, p. 107, lines 1-7.

[21] Transcript - Volume 2, p. 114, lines 21-26.

[22] Transcript - Volume 2, p. 138, lines 10-15.

[23] Transcript - Volume 2, p. 140, lines 8-17.

[24] Transcript - Volume 2, p. 146, lines 5-17.

(d) The FEU's internal controls regarding data security are reviewed by third parties on an annual basis.[25] The review performed by these third parties includes penetration tests that involve the third party attempting to penetrate the FEU's internal systems; review of the potential for access through the FEU's websites; review of access levels by customers; review of access levels to hosted environments; review of change control documents to ensure that the FEU's change control protocol is followed; and review of the FEU's encryption.[26]

(e) Although the FEU have stated that they typically do privacy impact assessments for projects involving a "significant" amount of personal information, the FEU confirmed that it will do a privacy impact assessment for any project involving sending personal information outside of Canada.[27]

(f) Security assessments are done for any technology project, regardless of scope or scale.[28]

(g) The FEU have never had a security breach.[29]

(h) The FEU have dedicated resources to data security whose job it is to ensure the security of the FEU's networks, whether from internal or external access. The FEU use the latest firewall protection, have active monitoring, and have intrusion prevention and detection mechanisms in place. The FEU use advanced products to assist with zero-day attacks.[30]

36. The FEU submit that the summary of key issues above and the discussions on these topics during the SRP support granting the order sought.

C. GOING FORWARD

37. Part of the FEU's presentation in the SRP was a summary of how the FEU will proceed going forward if the alternative relief is granted. The key components of how the FEU will proceed if it is permitted to store data outside of Canada, are the following:

---

[25] Transcript - Volume 2, p. 150, lines 3-8.

[26] Transcript - Volume 2, p. 176, line 13 to p. 177, line 7.

[27] Transcript - Volume 2, p. 154, lines 19-25.

[28] Transcript - Volume 2, p. 165, lines 12-14.

[29] Transcript - Volume 2, p. 169, lines 12-13.

[30] Transcript - Volume 2, p. 181, line 17 to p. 182, line 12.

(a) If the order is granted, the FEU will continue to apply the same rigor around security and privacy as are in place today. The FEU have never had a security breach.[31]

(b) The FEU will perform privacy impact assessments and security assessments for all projects that involve the storage of FEU data outside of Canada. The FEU have repeatedly stated that projects that do not meet the FEU's rigorous privacy and security standards simply will not go ahead.

(c) The FEU will encrypt or de-identify all customer, sensitive and FEU employee information before it leaves the FEU's security network.

(d) Encryption and de-identification keys will remain in Canada and at the FEU's data center at all times.

(e) All vendors in foreign jurisdictions who store data for the FEU will be contractually required to meet the FEU's privacy and security requirements.[32]

38. The FEU submit that these measures appropriately address the concerns raised in this proceeding, and support granting the order sought.

D. BENEFITS

39. The other aspect of "going forward" is the potential for the FEU and its customers to achieve meaningful benefits.

40. The detailed discussion of potential customer benefits is found in Section 5.2 of Exhibit B-8, the FEU's Evidence on the Proposed Alternative Relief. There, the FEU provide 5 examples of services that the FEU cannot now access, and that can provide meaningful customer benefits. These are examples for the purpose of illustrating the kind of benefits that the FEU are seeking to obtain.

(a) Example 1 is a product called Microsoft Azzure - the FEU estimate that the ability to use this product could reduce operating costs by approximately $100,000 annually. As noted above, the fact that Microsoft is establishing data centres in Canada does not necessarily mean that the FEU will be able to use these centres,

---

[31] Transcript - Volume 2, p. 169, lines 12-13.

[32] Ex. B-13, slide 12.

as latency may require the FEU to access these products through Microsoft's U.S. data centres.

(b) Example 2 is the Microsoft Office 365 product, which the FEU estimates could result in savings of $250,000 per year.

(c) Example 3 discusses human resource management tools that, if used, could result in the potential to save $1,000,000 in capital, and $200,000 to $400,000 annually.

41. Other examples are provided as well.[33]

42. The FEU submits that a consideration of these benefits further supports granting the relief sought.

E. CONCLUSION

43. For the reasons described in these submissions, the FEU submit that the Data Restriction should be removed, and the modified alternative relief granted, so that the FEU can pursue technology solutions that will benefit customers.

ALL OF WHICH IS RESPECTFULLY SUBMITTED.

Dated: June 30, 2015

[original signed by David Curtis]
David Curtis
Counsel for FortisBC Energy Utilities

[33] Ex. B-8, section 5.2.