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

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

December 18, 2014
File No.: 240148.00715/15951

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 Regulatory Timetable set for this proceeding, we enclose for filing the FEU's Reply Argument submission.

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

Reply Submissions of FortisBC Energy Utilities

December 18, 2014

TABLE OF CONTENTS

PART ONE: INTRODUCTION

1. These reply submissions address the final arguments of the Commercial Energy Consumers Association of British Columbia (CEC), the B.C. Sustainable Energy Association and Sierra Club British Columbia (BCSEA-SCBC), and the British Columbia Old Age Pensioners Organization *et al*. (BCOAPO).[1]

2. These reply submissions address the issues identified by the interveners as follows:

(a) **Part Two, Section A** addresses the general and unproven assertion of BCSEA-SCBC and BCOAPO that the storage of data outside of Canada is inherently risky;

(b) **Part Two, Section B** addresses comments about "public concerns";

(c) **Part Two, Section C** addresses the submissions of interveners regarding the appropriateness of the BC Privacy Commissioner considering privacy concerns (if and when they are raised);

(d) **Part Two, Section D** addresses the submissions of the interveners regarding the fact that technology has advanced since 2005 and customers should benefit;

(e) **Part Two, Section E** addresses the submissions of the interveners regarding the issue of the Data Restriction and inconsistencies; and

(f) **Part Three** is the FEU's conclusion.

3. For the reasons described in the FEU's submissions and these reply submissions, the FEU submit that the Data Restriction should be removed, so that the FEU can pursue technology solutions that will benefit customers.

4. The FEU submit, in the alternative, that the Data Restriction be rescinded, and a new data restriction order be made that only applies to customer "personal information" as defined in section 1 of the *Personal Information Protection Act*, S.B.C. 2003, c. 63.[2]

---

[1] In these reply submissions the FEU continue to use the terms defined in their initial submissions.

[2] That is, the revised data restriction would only require that customer personal information be stored on servers located within Canada.

PART TWO: REPLY SUBMISSIONS

A. BCSEA-SCBC's and BCOAPO's General Position Is Not Supported

5. BCSEA-SCBC and BCOAPO both oppose the application. At the core of BCSEA-SCBC's submissions is the notion that there is a "loss of security and privacy inherent in locating data/servers outside of Canada".[3] BCOAPO shares a similar notion. It says that "storing data and servers in a foreign jurisdiction puts the privacy rights of ratepayers at great risk".

6. The FEU have provided evidence in this proceeding that:

(a) As part of the assessment process of any proposal/project that will have a significant involvement with the collection, use or disclosure of personal information, the FEU will perform a Privacy Impact Assessment.[4]

(b) For all initiatives, a Threat Risk Assessment will be performed based on the type of initiative.[5]

(c) External providers will be subject to a complete risk assessment, as well as the terms and conditions regarding the FEU requirements for reliability and security.[6]

(d) Regardless of whether the data/servers are to be outside or inside Canada, third parties are (or future vendors will be) contractually required to meet and/or exceed the FEU's control environment for security of its enterprise wide network architecture and infrastructure. Contractual obligations will require control validation independent of the third party vendor and a report the findings to the FEU.[7]

(e) The FEU have implemented a control environment for security of its enterprise wide network architecture and infrastructure. This includes physical and logical security systems and control components including ensuring applicable government laws and regulations pertaining to minimum security control requirements are met. Third parties are contractually required to meet and/or

---

[3] BCSEA Submission, p. 2 of 5.

[4] Ex. B-3, BCUC IR 1.2.8.

[5] Ex. B-3, BCUC IR 1.3.2.

[6] Ex. B-3, BCUC IR 1.3.1.

[7] Ex. B-3, BCUC IRs 1.3.3.1 and 1.3.3.2.

exceed the FEU's control environment. A security breach is therefore not impacted by the physical location of the FEU's data.[8]

7. The FEU ask the Commission to accept the FEU's evidence that they will take the steps described above to protect customer information, and to reject the unsupported assertions of BCSEA-SCBC and BCOAPO that storing data outside of Canada results in an inherent loss of privacy, or that it puts customer data "at great risk". Most of the submissions of these interveners flow from these unsupported assertions, and should similarly be rejected.

B. Comments About Public Concerns

8. CEC points to the fact the Commission received a significant number of letters expressing concerns about privacy, foreign ownership of data, and control of data when KMI applied to acquire the Terasen Utilities in 2005.[9] It says that this evidence from 2005 may be considered evidence of considerable customer concern regarding foreign access to customer information. CEC also says that "there could be customers with legitimate concerns regarding access by foreign governments and this should be resolved as they do not have the option of selecting another service provider".[10]

9. In this proceeding not a single letter of comment has been filed by a member of the public, despite the fact that notice of the application was provided to, among others, all those parties who were registered as interveners and interested parties in the 2005 KMI proceeding. With respect, the complete absence of letters of comment from members of the public in this proceeding supports the conclusion that customers are less concerned about "foreign access" because the factor of direct foreign ownership is now removed.

C. The Appropriate Role of the BC Privacy Commissioner

10. BCSEA-SCBC submits that the argument that the BC Privacy Commissioner is the most appropriate tribunal to consider privacy concerns does not address the concern of storing

---

[8] Ex. B-3, BCUC IR 1.2.9.

[9] CEC Submission, p. 5.

[10] CEC Submissions, p. 7.

data in a foreign jurisdiction.[11] BCSEA-SCBC further submits that the fact that *PIPA* and *PIPEDA* permit private sector organizations to store data outside of Canada is "irrelevant to the Data Restriction, which is a condition imposed in the public interest under the *Utilities Commission Act*". The FEU disagree with these submissions. The provincial legislature has made a distinction between private sector organizations, such as the FEU, and public bodies: the former are permitted under provincial privacy legislation to store data outside of Canada, while the latter (public bodies) are not. This legislative intent demonstrates that there is nothing contrary to the public interest in allowing the FEU, as private sector organizations regulated under *PIPA* and *PIPEDA* as applicable, to store data outside of Canada. In doing so they are subject to the provisions of *PIPA* and subject to the regulatory oversight of the BC Privacy Commissioner and the federal commissioner. The FEU submit that the issue of foreign access to data stored outside of Canada is a matter that is addressed during the privacy impact assessment process; where the risks under consideration are unacceptable, the data will not be stored outside of Canada.

11. BCOAPO submits that the FEU ignore "the special nature of monopoly utilities as compared to other private sector companies and the broad mandate of [sic.] Commission".[12] They go on to make specific submissions in this regard (the bullet points that start on p. 3). BCOAPO's first submission under this topic is that there is something unique about the privacy issues faced by a public utility due to its "monopoly" status.[13] However, BCOAPO does not say what this status means in terms of privacy issues, or explain why the BC Privacy Commissioner is not an appropriate tribunal to regulate the collection, use and disclosure of personal information by the FEU. BCOAPO does not explain what, if anything, is added in terms of regulatory protection or efficiency by having the Commission also regulate this subject matter. The FEU submit, with the greatest respect, that the BC Privacy Commissioner is the appropriate regulatory body to address the FEU's collection, use and disclosure of personal information, and that BCOAPO has not explained why the FEU's status as a public utility should change this.

---

[11] BCSEA Submission, p. 3 of 5.

[12] BCOAPO Submission, para. 14.

[13] BCOAPO Submission, para. 14, first bullet.

12. BCOAPO's second submission under this topic is that the Commission does not only deal with "accounting, economic, finance and engineering".[14] The FEU agree that the description of the Commission's expertise in the 1996 *BC Hydro* decision is not necessarily exhaustive. However, the FEU submit that there cannot be any meaningful debate that the BC Privacy Commissioner has significantly greater expertise in dealing with privacy issues than the Commission.

13. BCOAPO's third submission under this topic is that only the Commission can properly weigh the costs and benefits of allowing the FEU to store data outside of Canada.[15] BCOAPO says "it is the role of the Commission to weigh the different factors against one another in order to evaluate the level of risk to the privacy of a ratepayer's personal information that is acceptable given the benefits that could result". With respect, there is nothing in the *Utilities Commission Act* that suggests that the Commission has any role to play in the regulation of privacy. The Commission's general supervision of public utilities is limited to matters such as:

(a) equipment,

(b) appliances,

(c) safety devices,

(d) extension of works or systems,

(e) filing of rate schedules, and

(f) reporting.[16]

14. The Commission has jurisdiction under section 44 of the *Utilities Commission Act* to make an order requiring a public utility to keep certain accounts or records in an office located in British Columbia. However, it is noteworthy that section 44 was included in the

---

[14] BCOAPO Submission, para. 14, second bullet.

[15] BCOAPO Submission, para. 14, third bullet.

[16] *Utilities Commission Act*, s. 23(1). Section 23(1) contains a more general statement of jurisdiction in 23(1)(g), however, that provision must be read against the items (a) through (f) that precede it, which have nothing to do with privacy or data storage.

original version of the *Utilities Commission Act* enacted in 1980, in the Act's predecessor the *Energy Act*, and was even included in the short-lived *Public Utilities Act* from 1919, which provided in section 7 that:

> Every public utility company shall have an office in the Province, in which it shall keep all such books, accounts, papers, and records as are required by the Commission to be kept within the Province. No company shall remove or permit to be removed from Province any book, account, paper or record so kept, except upon such conditions as may be prescribed by the Commission.[17]

15. The history of this provision suggests that it was not enacted with any notion of the storage of electronic information in mind, and it is unlikely that it was enacted with any notion regarding the protection of "personal information" or customer privacy. These concepts would have been foreign to the legislature in 1919, when this provision was first enacted.

16. In support of its submissions, BCOAPO cites an article written by "a group of law professors".[18] The meaning of the excerpt is difficult to discern from the fragment provided by BCOAPO. However, BCOAPO's only comment on the article is that "storing data in a foreign jurisdiction is a complex exercise that requires a full assessment". The FEU agree. As noted in the FEU's response to BCUC IR 1.2.8, as part of the assessment process of any proposal/project that will have a significant involvement with the collection, use or disclosure of personal information, a Privacy Impact Assessment will be performed.

D. Technology Has Advanced Since 2005 and Customers Should Benefit

17. BCSEA-SCBC says that the Data Restriction does not prevent the FEU from implementing cost-saving technology because the FEU can seek and obtain approval to locate data/servers outside Canada for specific purposes.[19] The FEU submit that this submission overlooks the purpose of the FEU's application. It is not efficient from a regulatory perspective for the FEU to have to bring discrete applications each time it wishes to store data outside of

---

[17] *Public Utilities Act*, S.B.C. 1919, c. 71, section 7. This Act was repealed in 1920, but it contains many of the same provisions that are found in the current UCA.

[18] BCOAPO Submissions, para. 18.

[19] BCSEA Submission, p. 4 of 5.

Canada. Furthermore, the FEU submit that if storage of data outside of Canada is a satisfactory way to proceed for specific proposals (as BCSEA-SCBC suggest), then the FEU can see no reason in principle why the removal of the Data Restriction in its entirety should be objectionable, so long as the FEU continue to employ the security measures described in the responses to IRs, such as vendor due diligence, network security and risk assessment.

18. BCOAPO submits that in the absence of a cost/benefit analysis of removing the Data Restriction, the application is premature.[20] CEC makes a similar submission.[21] These submissions miss the point of the Application. The FEU wish to have the Data Restriction removed so that they can explore cost saving projects and initiatives, safe in the knowledge that they can be carried out. There are numerous vendors who offer solutions and software that might not be available in Canada as they are often non-Canadian entities and will store data on servers outside Canada.[22] Having to apply for an exemption from the Data Restriction each time a project or initiative is contemplated will be inefficient and costly for customers, and there will be no incremental benefit in doing so.[23]

E. The Data Restriction and Inconsistencies

19. BCSEA-SCBC says that the Data Restriction is just one of "innumerable inconsistencies" between the FEU and other private sector organizations that are not regulated public utilities.[24] BCOAPO makes a similar submission.[25] Neither BCSEA-SCBC nor BCOAPO explain why the FEU's status as a public utility justifies the FEU being treated differently than other private sector organizations when it comes to matters of personal information and privacy. The FEU submit that there is no relevant difference, and that they should be permitted to store personal information outside of Canada, as other private sector organizations are lawfully permitted to do under *PIPA*.

---

[20] BCOAPO, paras. 28 to 30.

[21] CEC Submission, pp. 3 to 5.

[22] Ex. B-3, BCUC IR 1.6.5.

[23] Ex. B-3, BCUC IR 1.6.4.

[24] BCSEA Submission, p. 4 of 5.

[25] BCOAPO Submission, para. 22.

20. With respect to the issue of whether FBC is subject to a similar restriction[26], as the FEU noted in the response to BCUC 1.8.1, FBC is not subject to a direction that is similar to the Data Restriction. The direction referenced by BCSEA-SCBC (and the BCUC in IR 1.8.1) was only directed to the storage of customer information as it relates to the AMI Project.

21. CEC notes that as a "public body" under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*), BC Hydro is required to store personal information in its custody or control in Canada. It says that "it is not unreasonable for the BCUC to consider the same customer issues and concerns for a regulated utility such as FEU as those for BC Hydro."[27] The FEU submit that the fact that private sector public utilities are *not* scheduled as public bodies subject to *FIPPA* supports the view that they should be permitted to store personal information outside of Canada (as permitted under *PIPA*).

PART THREE: CONCLUSION

A. Summary of Position and Conclusion

22. The opposition to this application by the interveners is grounded in their unsupported belief that storing data outside of Canada is inherently risky. For the reasons stated above, this general proposition should be rejected.

23. The FEU do not have a panacea for all of the privacy concerns that are alive in our society today, or answers to the "Edward Snowden revelations".[28] The FEU should not have to bear the impossible onus of addressing all of society's privacy concerns in order to have the Data Restriction removed. The FEU have brought this Application so that they can be permitted to do what other private sector organizations in British Columbia are lawfully permitted to do under *PIPA*.

---

[26] BCSEA Submission, p. 4 of 5 and 5 of 5; BCOAPO Submission, paras. 22 to 26.

[27] CEC Submission, p. 4.

[28] BCOAPO Submission, para. 19.

24. The FEU have explained how they will approach managing privacy related risk, and can assure the Commission and interveners that where the risks are unacceptable the FEU will not take those risks.

25. The FEU's intentions are to achieve cost savings and to avoid losing those savings in repeated applications to the Commission on discrete projects. These are worthy intentions.

26. For the reasons described in the FEU's submissions and these reply submissions, the FEU submit that the Data Restriction should be removed, so that the FEU can pursue technology solutions that will benefit customers.

B. Alternative Relief

27. Having reviewed the submissions of the interveners, the FEU believe that the primary, if not sole concern raised in this proceeding has been with the privacy and security of customer information.

28. For this reason, the FEU submit that if the Commission does not grant the relief sought by the FEU, then the Data Restriction should be rescinded, and replaced with an order that:

(a) directs that FEU data of or about customers that meets the definition of "personal information" under *PIPA* must be stored on servers located within Canada;

(b) permits the FEU to store data about customers that would otherwise meet the definition of "personal information" outside of Canada if it is either (a) de-identified or (b) encrypted;

(c) confirms that data of any kind, customer or otherwise, that does not meet the definition of "personal information" under *PIPA* is permitted to be stored outside of Canada; and

(d) permits the FEU to apply for specific exemptions from the revised Data Restriction.

29. This revised data restriction would permit the FEU to store other types of data on servers outside of Canada, while addressing the concerns voiced in this proceeding.[29]

30. The FEU submit that such an approach is a reasonable way to address the concerns of the interveners, while allowing the FEU to achieve cost savings for the benefit of customers, should the Commission not grant the full relief sought by the FEU.

ALL OF WHICH IS RESPECTFULLY SUBMITTED.

Dated: December 18, 2014 ***[original signed by David Curtis]***

David Curtis
Counsel for FortisBC Energy Utilities

[29] Something like this alternative relief appears to be what CEC supports in its submission, where it says: "if the data location restriction is to be removed that FEU be directed to establish a process or procedure that would shield customer information from foreign government access. Such shielding could occur by way of alternate storage options (i.e., in Canada), removal of identifiers if suitable or other method recommended by FEU IT specialists and approved by the Commission" - CEC Submission, p. 3. Also see CEC's comment at p. 2 that "the CEC is not specifically opposed to allowing data to be stored outside of Canada if suitable protections are in place to prevent foreign government access".