IN THE MATTER OF AN ARBITRATION UNDER CHAPTER ELEVEN OF THE NORTH AMERICAN FREE TRADE AGREEMENT AND THE UNCITRAL ARBITRATION RULES

BETWEEN:

TENNANT ENERGY LLC

Investor

AND

GOVERNMENT OF CANADA

Party

INVESTOR'S SUBMISSION ON CONFIDENTIALITY
April 23, 2019

Appleton & Associates International Lawyers
77 Bloor St. West, Suite 1800
Toronto, ON M5S 1M2

Reed Smith LLP
1001 Brickell Bay Dr., 9th Floor
Miami, Fl 33131

1. The regulation of digital innovation has added a new dimension to the discussion of confidentiality. This submission considers the impact of mandatory data privacy rules that apply to this arbitration because of the participation of persons subject to mandatory EU data protection rules.

2. The Investor notes that the disruptive application of these European Union data privacy rules commenced in May 2018. The application of EU rules in a NAFTA Arbitration was not anticipated at the commencement of the arbitration. The appointment of at least one arbitrator subject to the EU rules makes a careful consideration of these rules necessary. The application of these mandatory rules affects the consideration of confidentiality, and other matters in the orderly conduct of international arbitration.

3. This submission stresses the need for the Tribunal to take measures to ensure that more information is obtained from all those involved in the arbitration (including the arbitrators, the administering institution and the disputing parties) before an applicable confidentiality order can be made. Deciding confidentiality before deciding the data privacy and security issues is putting the cart before the horse.

4. There is a need for the participants in this arbitration to first sort through the data privacy aspects of the confidentiality issue. Logically, the terms, scope, and coverage of the Confidentiality Order follow the determinations to be made by the Tribunal on privacy, which must be based on obtaining additional information to design and implement a workable approach.

5. Two days after the Investor filed its submission on data privacy of April 16th, the Investor invited Canada to take is concerns over EU Data Privacy and Security concerns into account by way of a new Confidentiality Order.[1] The draft provided by Canada is entirely inadequate to address these concerns as well as having other problems with are addressed later in this submission.

---

[1] The April 18, 2019 email from Barry Appleton to Lori Di Pierdomenico included the following:

> "We have received your email today concerning your modified confidentiality order. Our submission of April 16th concerning data privacy and the impact of the GDPR has important impacts on the process to manage confidentiality in this arbitration. Also, our email correspondence of February 20, 26 and 27, 2019 is also relevant to the issues of the treatment of confidential information.
>
> Your email from earlier today indicates that your modified Confidentiality Order differs "subject to a few corrections and edits."Considering the serious issues raised in our correspondence, a different approach is needed. We are disappointed that your client has not considered any of the information exchanged between the parties since the making of your original proposal. We cannot see how this issue can be resolved through minor wording variances to your original proposal.
>
> Making an order before deciding data privacy is putting the cart before the horse. It would be much more helpful first to sort the data privacy side of confidentiality. Logically, the confidentiality order follows the decisions on privacy."

6. Canada did not respond to the Investor's invitation to modify the proposed order.The Investor submits that with careful thought and full disclosure of necessary information, it should be possible to apply the GDPR in a manner that is consistent with the obligations in NAFTA Article 1115 and UNCITRAL Article 15. The Investor underscores however that considerable forethought is necessary. The draft order proposed by Canada cannot meet the needs of what is necessary

7. As outlined below, the Investor sets out the following in this submission:

    a. The need to obtain more information from the participants in this arbitration (namely the arbitrators, the PCA, and the disputing parties) before the making of a Confidentiality Order;

    b. Identifying ways to establish procedural orders that will permit the orderly unfolding of the arbitration and will be consistent with applicable data privacy and protection legislation.

    c. Addresses concerns concerning proportionality and burden which go outside of the data privacy and protection sphere.

I. <u>The need to address Data Privacy and Security</u>

8. On April 16, 2019, the Investor provided observations on the issue of Data Privacy and Security. These questions arise primarily because of the mandatory application of the EU General Data Privacy Regulation (GDPR) to persons involved in this arbitration. The provisions of the GDPR came into effect in May 2018, and thus present questions of first impression to international arbitrations.

9. The Investor appended a draft Task Force report prepared by the International Bar Association ("IBA") and the International Council on Commercial Arbitration ("ICCA") on the specific issue of the best practices for international arbitration tribunals affected by the EU GDPR.[2]

10. The IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration RoadMap (the "RoadMap") discusses the meaning of data privacy and protection for international arbitration. The introduction to the RoadMap identifies the complicated task for tribunals to balance the obligations of the General Data Protection Regulation along with the fundamental objectives of arbitration. The RoadMap states:

> Arbitration plays a major role in the administration of justice in cross-border disputes. Moreover, the processing of personal data (by means of communication,

[2] The Investor provided a draft consultation copy of the joint IBA-ICCA Task Force on Data Privacy in International Arbitration. The draft report was obtained at the IBA International Arbitration Day on March 23, 2019. Its release is expected shortly. (**C-1**)

> as well as documentary and witness evidence) is an essential component of the arbitral process. The consensual nature of arbitration, the independence of arbitral decision-making and the secrecy of deliberations are fundamental tenets of the arbitration process. Applying the GDPR to arbitration therefore requires balancing the rights and obligations contained in the GDPR with the fundamental rights of defence and due process at stake in every arbitration (Art. 24).[3]

11. The GDPR obligations have an impact on the shape and content of a confidentiality order. The GDPR applies whenever personal data is processed in the EU. Personal Data means information in relation to a person who can be directly or indirectly identified from that information.[4] Article 4(7) of the GDPR provides that a data controller is the person who decides why and how personal data is processed. The GDPR imposes obligations on data controllers. Arbitrators, legal counsel, and witnesses generally would fit within the definition of data controllers. Joint controllers are those who jointly control the "purpose and means" of the data processing. This would cover the Tribunal. The disputing parties would also fit within this coverage whenever they jointly agree on the purpose and means of data processing such as through a consent order. Joint controllers are jointly and severally liable for data protection violations under the GDPR.

12. Because of this broad coverage and the serious penalties for non-compliance, it is essential that the Confidentiality Order be carefully considered.

13. The *Debevoise Protocol to Promote Cybersecurity in International Arbitration* suggests that the tribunal consider appropriate protocols and procedures "usually in the first procedural conference: The *Debevoise Cybersecurity Protocol* states:

> 1. We will request that the arbitral tribunal establish protocols and procedures for the transfer of sensitive information at the outset of proceedings, usually in the first procedural conference. What constitutes such sensitive information should be defined in light of the particular circumstances of a dispute.
>
> a. These protocols and procedures may include: (i) defining categories of sensitive information, updated as necessary through the course of the proceeding; and (ii) agreeing on processes for the secure transfer of such sensitive information between and among the tribunal and the parties.[5]

14. The IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration Explanatory Notes has set out a three-part test concerning the application of the GDPR to arbitrations:

---

[3] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration – Introduction (**C-2**).

[4] GDPR Article 4. (**C-2**)

[5] Debevoise Protocol to Promote Cybersecurity in International Arbitration (**C-5**), available at https://www.debevoise.com/~/media/files/capabilities/cybersecurity/protocol_cybersecurity_intl_arb_july2017.pdf

a. Is there an 'establishment' in the EU within the meaning of EU data protection law,

b. Is there 'processing in the context of the activities of an establishment in the Union,'

c. Is there an exception to the obligations? If not, how can data be lawfully transferred?

15. If the GDPR applies to the arbitration, then there needs to be a subsequent analysis of how GDPR obligations will affect confidentiality, data protection and data privacy in the arbitration.

16. The failure to comply with the GDPR could result in substantial fines, criminal sanctions against the data controllers and those who control jointly with them (on a joint and several basis) and the risk of civil liability.[6]

A. Confirming an Establishment in the EU?

17. On these preliminary questions, the IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory Notes referred to decisions of the European Data Protection Board ("EDPB") and its predecessor – the Section 29 Working Party. The RoadMap Explanatory Notes state:

> **1. Arbitral Participants with an EU establishment**
>
> In deciding whether the GDPR applies, the first question an Arbitral Participant needs to ask is whether they have an EU establishment. In this respect, the EDPB clarified in the Draft Territorial Guidance that this question requires a three-fold analysis and that the application of the establishment criterion should be considered "*first by considering the definition of an 'establishment' in the EU within the meaning of EU data protection law, second by looking at what is meant by 'processing in the context of the activities of an establishment in the Union', and lastly by confirming that the GDPR will apply regardless of whether the processing carried out in the context of the activities of this establishment takes place in the Union or not.*"
>
> The EDPB recommended that this three-fold analysis should be undertaken in the context of the specific processing activities at issue and taking into account whether the data custodian is properly considered a data controller or a data

[6] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration – I. I. GDPR for Arbitration in a Nutshell --f. Supervision and sanctions (**C-2**)

processor with respect to those processing activities. [7]

B. Establishment of a stable relationship in the EU

18. The IBA-ICCA Task Force Explanatory Notes address the test for establishment. This test is not defined in the GDPR but has been established in EU law. The European Data Protection Board (EDPB) and the European Court of Justice have both given broad meaning to this term, and the contexts for its coverage. The IBA-ICCA Task Force Explanatory Notes say:

> *i. Establishment*
>
> As recognized by the EDPB, what constitutes an establishment is not defined in the GDPR. The EDPB's discussion of what constitutes an establishment is worth quoting:
>
> > While the notion of "main establishment" is defined in Article 4(16), the GDPR does not provide a definition of "establishment" for the purpose of Article 3. However, Recital 22 clarifies that an "*[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect*."
>
> This wording is identical to that found in Recital 19 of Directive 95/46/EC, to which reference has been made in several CJEU rulings broadening the interpretation of the term "establishment," departing from a formalistic approach whereby undertakings are established solely in the place where they are registered. Indeed, the CJEU ruled that the notion of establishment extends to any real and effective activity — even a minimal one — exercised through stable arrangements. In order to determine whether an entity based outside the Union has an establishment in a Member State, both the degree of stability of the arrangements and the effective exercise of activities in that Member State must be considered in the light of the specific nature of the economic activities and the provision of services concerned. (footnotes omitted).[8]

---

[7] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory notes at Explanatory Note 4 – Section 1 – Arbitral Participants with an EU establishment (**C-3**).

[8] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory notes at Explanatory Note 4 – Section 1 – Arbitral Participants with an EU establishment (i) establishment. Here the Task Force is making reference to Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, European Data Protection Board, (2018) ("Draft Territorial Guidance"). (**C-3**).

19. The IBA-ICCA Task Force concludes that:

> Applying this standard, in deciding whether they are established in the EU, Arbitral Participants should consider whether they undertake activities in the EU through "*stable arrangements*," regardless of the legal form those arrangements take.[9]

C. Is there 'processing in the context of the activities of an establishment" in the EU?

20. Article 3 of the GDPR provides as follows:

> 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.[10]

21. The IBA-ICCA Task Force summarizes the effect of Article 3 as follows:

> *Scope of GDPR's Application to EU Establishments*
>
> Article 3(1) of the GDPR states expressly that if the data is processed in the context of the activities of an EU establishment it applies "*regardless of whether the processing takes place in the Union or not*." Therefore, the EDPB emphasizes that "*[i]t is the presence, through an establishment, of a data controller or processor in the EU and the fact that a processing takes place in the context of the activities of this establishment that trigger the application of the GDPR to its processing activities. The place of processing is therefore not relevant in determining whether or not the processing, carried out in the context of the activities of an EU establishment, falls within the scope of the GDPR.*" [11] 7

22. The IBA-ICCA Task Force continues:

> Applying these criteria, Arbitral Participants would typically consider first, whether they are undertaking activities in the EU through stable arrangements, and, if so, whether the data processing activities at issue are being carried out in the "*context*" of those activities. If the answer to both questions is affirmative, those data processing activities are covered by the GDPR.

---

[9] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory notes at Explanatory Note 4 – Section 1 – Arbitral Participants with an EU establishment (i) establishment (**C-3**).

[10] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory notes at Explanatory Note 4 (**C-3**).

[11] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory notes at Explanatory Note 4 – Section 1 – Arbitral Participants with an EU establishment (iii) Scope of GDPR's Application to EU Establishments (**C-3**).

This will not always be straightforward. For example, where arbitrators from outside the EU have tenancy arrangements with chambers within the EU, such arrangements arguably qualify as a stable establishment. The issue that such arbitrators should focus on in their analysis is whether the data processing they engage in is being undertaken in the context of the activities of their chambers in the EU or not.[12]

D. Exceptions:

23. As noted in the April 16, 2019 submission on data privacy, the EU has not issued any exceptions to arbitration tribunals similar to the court exception.

24. Also, a panel at the March 2019 IBA Arbitration Day confirmed that the national data privacy authorities in the United Kingdom have confirmed to a delegation of arbitrators from the LCIA that the UK has not issued, and is not inclined to issue an exception to the GDPR for arbitration.

E. Establishment and Context: Application to the present arbitration claim:

25. We understand that Arbitrator Bethlehem has a stable relationship in an EU member state.[13] Thus the territorial connection applies to his involvement in this arbitration, and this connection provides the context necessary for the application of the GDPR.

26. While it would initially appear as if the other parties to the arbitration are not individually covered by the GDPR, the following factual establishment questions need to be canvassed:[1]

- Are the disputing parties, the arbitrator or the PCA offering services (defined in the GDPR as "targeting data subjects") in the EU? If so, the members of the tribunal and the disputing parties have to designate an EU resident for GDPR purposes under Art 27.

- We need additional information to determine whether Canada, Arbitrator Bull or Arbitrator Bishop have a "stable relationship" in the EU.

(This determination is without regard to the subsequent question of coverage through joint control, which may also impose obligations upon those who are outside of the EU)

---

[12] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory notes at Explanatory Note 4 – Section 1 – Arbitral Participants with an EU establishment (iv) Application to Arbitral Participants (**C-3**)

[13] (See IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory Notes at Explanatory Note 1 - section 2 - Arbitral Participants without an EU Establishment (**C-3**).

27. One essential question is that a confidentiality order will need to address personal data processing, sensitive data processing, and data protection.[14]

    a. Communications with Arbitrator Bethlehem constitute a transfer of data across an international frontier (that is into, or outside of, the EU). Such transactions trigger GDPR obligations every time a transfer occurs. Because of the supranational status of the Permanent Court of Arbitration, data transfers to and from the PCA to Arbitrator Bethlehem are an international transfer and thus trigger the international responsibilities;

    b. The Tribunal will need to confirm that it lawfully can process data. The IBA-ICCA Task Force identify that informed consent can only come from the data subjects themselves and not from the Arbitration Participant (that is the disputing parties).[15] The parties and Tribunal need to determine, based on the facts of the situation, whether there is a legitimate interest for the data controller in processing the personal data.

    c. The Arbitrators and disputing parties will require information from the PCA to confirm whether all data sent or maintained by the PCA is stored and processed entirely on premises subject to the PCA Headquarters Agreement. Should there be transfers outside of the territory covered by the Headquarters Agreement, then this would affect GDPR compliance.

    d. Deliberations made by the Tribunal in Europe made outside of the territory of the PCA (covered in its Headquarters Agreement) would also trigger GDPR requirements independently;

    e. The disputing parties themselves would not trigger GDPR obligations in transfers of data *inter se.*

    f. We have no information about whether Canada has engaged counsel or experts who would trigger GDPR requirements. Furthermore, we do not know if there would be witnesses who would trigger GDPR requirements in Europe.

    g. At this point, the Investor has not engaged experts or counsel who trigger GDPR requirements, but counsel for the Claimant has an office in London which may become involved in this matter.

28. The obligations under the GDPR concerning confidentiality apply on account of obligations arising due to the processing of personal data. The Task Force Explanatory Notes address the nature of personal data as follows:

---

[14] IBA-ICCA Task Force on Data Privacy in International RoadMap at Section III(c) – *lawfulness of processing personal Data, Sensitive Data and Data Transfers.* (**C-2**)

[15] IBA-ICCA Task Force on Data Privacy in International RoadMap at Section III(c) – *lawfulness of processing personal Data, Sensitive Data and Data Transfers* and sections immediately following (**C-2**).

"*Personal data*," is defined as any information relating to an identified or identifiable natural person, who is referred to as the "*data subject*." It is wider than the US concept of Personally Identifiable Information or PII.

An identifiable person is one "*who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*" (Art. 4(1)). The EU does not distinguish between information that arose in a business or non-business context. As long as an individual is, or could be, identified through the information provided, and irrespective of whether that information is contained in a single document or any combination of documents, data qualifies as personal. For the purposes of data protection, the ordinary meaning of what is considered to be "*personal*" is wholly inadequate.

As a result, business and non-business-related information (including technical data like cookies and IP addresses) submitted as evidence or contained in written pleadings would be covered whenever an individual is named, or his or her identity could be derived. Therefore, while the evidence submitted and exchanged is typically thought of as being the source of potential data protection concerns, the memorials, witness statements, expert reports, and the award itself are also likely to identify individuals and to be covered. Information that is clearly "*about*" someone is also likely to constitute personal data. That includes opinions or assessments (for example, as to their credibility as a witness), whether subjective or objective, true or false. Much of the data exchanged during a typical international arbitration contains information qualifying as personal data in the sense of the GDPR.

> Example: An arbitrator appointed in a case sends an email to her co-arbitrators containing the sentence "*I don't think that Mr. Johnson was a particularly good witness.*" Mr. Johnson's name, and the arbitrator's opinion of him, each fall within the definition of "*personal data*." If the GDPR applies, that data must be processed by each of the arbitrators appropriately, including the data transfer provisions.[16]

[16] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory Notes at Explanatory Note 5 - What "personal data" is processed during an arbitration (**C-3**).

29. This Tribunal will need to consider the various types of roles that participants in the arbitration could play, and thus the modalities in which witnesses, experts, the Tribunal members, parties and even third parties trigger obligations.[17]

30. The scope of covered data is exceedingly broad. The IBA-ICCA Task Force Explanatory Notes address situations when personal data is "processed" during an arbitration. The Task Force states:

> Under that expansive definition, much of the data involved in the performance of activities typically undertaken during the arbitral process relating to submissions and evidence qualify as personal data, the processing of which must comply with the GDPR requirements. For example, the following activities would likely constitute the processing of personal data:
>
> • Receipt of documents;
>
> • Exchange of emails;
>
> • Document review;
>
> • Drafting written submissions;
>
> • Document transfer to a third party engaged to assist during the process, including external providers of electronic data review services, court reporters, interpreters, external counsel, or an independent expert engaged by a party;
>
> • Disclosure of materials during the arbitral process to the other party, their counsel or expert, the arbitral institution or the tribunal (e.g. document disclosure, submitted evidence, witness statements, expert reports, memorials);
>
> • Tribunal-ordered disclosure of materials;
>
> • Preparation, drafting, exchange and issuance of an award;
>
> • Transcriptions, audio- and video recordings of hearings;
>
> • Document retention; and

[17] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory Notes at Explanatory Note 13 - Who acts as a data controller versus a data processor during an arbitration? (**C-3**).

• Document destruction.[18]

31. Previous international arbitration tribunals have not had to consider the GDPR and have not addressed these considerations. The Tribunal will need to consider GDPR in terms of evidence provided to the Tribunal and in terms of how the tribunal processes such evidence. Obligations arise in how this confidential information is:

    a. Handled;

    b. Considered;

    c. Made public;

    d. Stored in a manner that protects against accidental loss, destruction or damage; and

    e. Eventually destroyed.[19]

32. To this end, the Tribunal in its Confidentiality Order should consider:

    a. The process of how evidence is gathered. The "purpose limitation" for data means that data is only used in the way of its original intention and for specific and limited purposes that need to be communicated to the data subject. The "processing" of this information by the Tribunal must be consistent with this initial intention under GDPR Art 5(1).[20] Otherwise, additional notices to the data subjects are necessary.

    b. The Tribunal should specify the content of data privacy notices, and mandate that they are posted by the disputing parties, the PCA and all affected arbitrators.

    c. The way data is used needs to be considered to take into account data minimization procedures to reduce may need to be notified to data subjects and to take adequate data security and confidentiality steps. Also, the process of data mapping appears to be a very useful initial step.[21] Data mapping describes planning the steps and data transfers in advance to ensure adequate steps are taken.[22]

---

[18] IBA-ICCA Joint Task Force on Data Protection in International Arbitration: RoadMap to Data Protections in International Arbitration - Explanatory Notes at Explanatory Note 6 - When is personal data "processed" during an arbitration? (**C-3**).

[19] IBA-ICCA Task Force on Data Privacy in International RoadMap, Section 1(d) – *Key Obligations* (**C-2**)

[20] IBA-ICCA Task Force on Data Privacy in International RoadMap at Section II(b) – *purpose limitation* (**C-2**)

[21] IBA-ICCA Task Force on Data Privacy in International RoadMap at Section II(b) – *data minimization*. (**C-2**)

[22] IBA-ICCA Task Force on Data Privacy in International RoadMap at Section II(b) – *data mapping*. (**C-2**)

33. Some orders made by previous NAFTA Tribunals arising before May 2018 (that is before the GDPR was applicable), addressed procedures for the "declassifying" of the confidential information through redaction to result in a public document and the production of confidential versions. Such approaches alone are not fully consistent with the GDPR.

34. The Tribunal must be vigilant about the treatment of personal privacy data. In the words of the *Debevoise Cybersecurity Protocol*:

> 8. We will explore with the arbitral tribunal whether sensitive information may be submitted in a form that is only screen viewable (i.e., not downloadable or printable). If sensitive information is permitted to be printed, we will ask the tribunal to establish consistent policies and procedures related to the destruction of printed materials.
>
> 9. To the extent practicable, we will limit the persons who have access to sensitive information to those persons having a need-to-know with respect to such information.[23]

35. The GDPR imposes a set of constraints upon the unlimited discretion of the Tribunal. An order to disclose information protected by the GDPR now requires consideration of matters which go outside of the considerations contained in the IBA Rules on the Taking of Evidence.[24]

36. The Investor submits that with careful thought and full disclosure of necessary information, it should be possible to apply the GDPR in a manner that is consistent with the obligations in NAFTA Article 1115 and UNCITRAL Article 15.

II. Ways to Address Data Privacy and Security

37. International organizations such as the Permanent Court of Arbitration or the World Bank, which are established under international law or by an agreement between countries, are treated as though they are outside the EU. This is through the operation of GDPR Article 4(26) and its definition of international organizations and the related Article 46(1) which governs data transfers to international organizations). Thus, the transfers of data to the PCA, the administrating body in this arbitration, is considered a transfer of data between an EU controller and someone outside the EU.

38. The IBA-ICCA Task Force carefully considered the basis for the lawful transfer of data between an EU controller and someone outside the EU. In this arbitration, transfers between Arbitrator Bethlehem, the rest of the Tribunal, the PCA and the Parties would trigger these rules.

---

[23] *Debevoise Protocol to Promote Cybersecurity in International Arbitration*, July 2017 (**C-5**)

[24] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 20- How does data minimization fit with the IBA Rules? (**C-3**)

39. The Task Force reports in the Explanatory Notes:

When can personal data lawfully be transferred outside of the EU?

The GDPR establishes rules for transfers of personal data to third countries by all Arbitral Participants, whether they be data processors or data controllers.

The GDPR allows third country data transfers where:

- The country has been deemed to provide adequate data protections;
- The data controller or data processor has put in place "*appropriate safeguards*" to protect the data in one of the means expressly prescribed by the GDPR; or
- One of a list of specified derogations apply, including where the processing is "*necessary for the establishment, exercise or defence of legal claims*" (Arts. 45-49).

Regardless of the means employed by a party to transfer personal data outside the EU, the recipient of the data must be required by law or by agreement to apply adequate protections to the data after its transfer, including the main principles of the GDPR (Art. 44). In the arbitration context, it is important to recall that international organisations such as the Permanent Court of Arbitration, the World Bank, and the International Court of Justice, which are established under international law or by an agreement between countries, are treated as though they are outside the EU (Art. 4(26) defining international organisations, Art. 46(1) addressing transfers to international organisations).

The EDPB has explained that the exceptions allowing data transfers follow a cascade approach, as follows:

- First, transfer may take place if there is an adequacy decision, allowing data transfers to the relevant country;
- Second, if data is to be transferred to a country without an adequacy decision, one of the expressly listed "*adequate safeguards*" must be put in place where feasible;
- Third, in case there is no adequacy decision and adequate safeguards are not feasible either, a specific derogation can be relied on; and
- Lastly, if none of the express derogations is applicable, a party may rely on its "*compelling legitimate interests*" as a basis for transfer, but this is a high standard and requires notification to the data subjects and the

supervisory authority.[25]

F. Adequacy Decisions

40. The EU has issued adequacy decisions which permit the transfer of data from the EU. Adequacy decisions permit transfers of information about EU citizens to companies in third countries without the need for additional safeguards or the need for foreign firms to individually show compliance with the GDPR. The following adequacy decisions could be relevant in this arbitration:

41. The EU has issued adequacy decisions to the United States for entities enrolled in the EU-US Privacy Shield). An entity that is not covered by the Data Shield is not covered by an Adequacy Decision.

42. The EU has only permitted the transfer of data to commercial organizations in Canada. The EU determined that Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) was providing adequate privacy protection. PIPEDA only applies to private sector companies and expressly does not apply to the Government of Canada and provincial governments.

    a. The Canadian law firm acting for the Investor is thus covered by PIPEDA and the existing EU Adequacy Decision.
    b. Since the Government of Canada is not covered by PIPEDA, data transfers to the Government of Canada do not have Adequacy Decision coverage (and safeguards are required).

43. Where there is an adequacy decision, the GDPR permits third country data transfers where appropriate safeguards are in place. However, where there is no adequacy decision, the GDPR requirements are more difficult to satisfy.

44. Data transfers from Arbitrator Bethlehem to most persons in this arbitration are not covered by existing adequacy decisions. This would include:

- Transfers with the President of the Tribunal based in Singapore (a country not on the Adequacy List);

- Transfers with the Respondent;

- Transfers to US-based persons such as arbitrator Bishop, the Investor, US-based counsel for the Investor at Reed Smith (both organizations not covered by the Privacy

[25] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 10- When can personal data lawfully be transferred outside of the EU? (**C-3**)

Shield) require strict compliance with adequate safeguards.

- Transfers with the Permanent Court of Arbitration (which is treated like a transfer outside the EU but where there is no existing Adequacy Decision). Such data transfers require strict compliance with adequacy safeguards.

45. The Investor also notes that the NAFTA provides for certain circumstances when data transfers of evidence can be made to others who are not parties to the arbitration, such as the non-Disputing NAFTA Parties under NAFTA Article 1129(1). Article 1129 (2) provides that:

> A Party receiving information pursuant to paragraph 1 shall treat the information as if it were a disputing Party.

Thus, the non-Disputing NAFTA Parties will also be required to comply with the GDPR requirements if either wish to obtain evidence filed in this arbitration. Such matters should be addressed in a procedural order, including the Confidentiality Order.

46. The IBA- ICCA Task Force Explanatory Notes provides a standard contractual clause that can be used. Such clauses must be adopted verbatim to comply with the EU regulations. The Task Force comments:

> The adoption of standard contractual clauses can be seen as effectively bringing the data protection standard up to the level of adequate protection between the entities adopting them, allowing data to transfer freely between them, although further transfers are not allowed without putting in place additional standard contractual clauses insuring protection after the onward transfer.
>
> The standard contractual clauses are promulgated by the EU and must be adopted verbatim. By adopting standard contractual clauses, the data exporter agrees to ensure the data meets a certain standard of treatment upon transfer out of the EU and the data importer agrees to comply with the main principles of EU data protection law after the transfer. The standard contractual clauses expressly set forth the applicable obligations imposed on the data importer in the text of the clauses and by way of an Annex.[26]

47. The standard clauses are available from the EU website.[27] The voluntary agreement to the EU standard contractual provisions is the easiest manner to permit lawful data transfers under this route.

---

[26] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 12 - what are Standard Contractual Clauses? (**C-3**)

[27] The standard clauses are available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

48. As an alternative, there is a limited occasional use derogation. An occasional transfer of data to a third country is permitted in pursuit of the arbitration when "necessary for the establishment, exercise or defense of legal claims" under GDPR.[28]

G. Data Security Concerns and Confidentiality

49. Explanatory Note 10 of the IBA-ICCA Task Force addresses the data security requirements in an arbitration. These issues are directly relevant to the issues of confidentiality in the arbitration. The IBA-ICCA Task Force reports:

> The GDPR requires all controllers and processors of personal data governed by its terms to implement appropriate technical and organisational measures to ensure a "*level of security appropriate to the risk*" (Art. 32). This means that whenever the GDPR applies to personal data processed in an arbitration, adequate data security is *mandatory*.
>
> Article 5(1)(f) of the GDPR concerns the "*integrity and confidentiality*" of personal data. It establishes the principle that personal data shall be:
>
> > [P]rocessed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
>
> Article 32 of the GDPR explains that the following measures are required to secure all data covered by its terms:
>
> 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:
>
> > a. the pseudonymisation and encryption of personal data;
> > b. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
> > c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
> > d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

---

[28] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 12 - **What does "*necessary for the establishment, exercise or defence of legal claims*" mean? (C-3)**

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. [29]

50. The Task Force continues by analyzing some of the obligations. In particular, the Task Force offers the following:

> The GDPR lists a number of mechanisms that may be employed to reach that appropriate level of security, none of which are required but that should be considered as appropriate:
>
> • ***Pseudonymisation and encryption –*** Pseudonymisation and encryption are specified in the GDPR as examples of measures that may be appropriate depending on the circumstances.
>
> • ***Confidentiality, integrity, availability, and resilience*** – The GDPR instructs Arbitral Participants to consider the basic principles of "*confidentiality, integrity and availability*" of the personal data they process. Sometimes referred to by data security professionals as the "*CIA triad*," confidentiality, integrity, and availability are three important elements of data security to be considered under the GDPR. Any data security measures employed by Arbitral Participants should endeavor to ensure these principles are complied with both with respect to their systems and the data processed.
>
> The GDPR also suggests that Arbitral Participants consider providing for "resilience" in their processing systems and services. The ICO has explained in its helpful guidance on this topic that resilience in this context refers to whether systems can continue operating under adverse conditions, such as those that may result from a physical or technical incident, and their ability to be restored to an effective state. [30]
>
> • ***Restore*** – The GDPR also asks Arbitral Participants to consider the ability of their systems to "*restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*." The GDPR does not define what a "*timely manner*" should be, but the ICO has suggested that this will depend on:
>
> • Who the data controller is;

[29] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 10 - what Data Security is required during an arbitration (**C-2**).

[30] *See Information Commissioner's Office, United Kingdom, Guide to the General Data Protection Regulation (GDPR), Security.* (**C-6**)

- What systems the data controller has; and

- The risk that may be posed to individuals if the personal data the data controller processes is unavailable for a period of time. [31]

51. Considering the coverage of the GDPR, the Confidentiality Order in this arbitration must be compliant with the obligations in GDPR Article 32.

52. While the issue of appropriate cybersecurity is associated with confidentiality, The IBA-ICCA Task Force addresses suggestions for cybersecurity for arbitration tribunals as follows:

> This reflects both the GDPR's risk-based approach, and that there is no "*one size fits all*" solution to data security as stressed in the ICCA/NY Bar/CPR Cybersecurity Framework for International Arbitration (2019).
>
> This means that what is "*appropriate*" will depend on many factors including the Arbitral Participant's function, the size and type of organization (including number of employees and its premises and data systems), the type of processing being undertaken and whether data processors are used), whether third party data transfer is required and if so, where, and the types of data being processed including how valuable, sensitive or confidential and the damage or distress that may be caused if the data was compromised.
>
> Important initiatives have been undertaken towards ensuring cybersecurity in international arbitration. These include the Debevoise & Plimpton Protocol to Promote Cybersecurity in International Arbitration launched in 2017, the ICCA/NY Bar/CPR Cybersecurity Framework for International Arbitration (2019) and the IBA Cybersecurity Guidelines (2018). While none of these initiatives address the data security requirements of the GDPR directly, they provide a useful resource for applying a risk-based analysis to cybersecurity, and the ICCA/NY City Bar/CPR Cybersecurity Framework for International Arbitration further provides a structure for how data protection may be addressed in international arbitration.[32]

53. Article 5 of the GDPR references the principle of data minimization. This principle should be carefully considered. The needless production of confidential information covered by the GDPR increases the risk to the arbitration participants.

54. Concerning information that is produced, Data Privacy Notices and Data Security are necessary elements for inclusion in the confidentiality order. The goal is to ensure that

---

[31] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 10 - what Data Security is required during an arbitration (**C-3**)

[32] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 10 - what Data Security is required during an arbitration (**C-3**); Debevoise Protocol to Promote Cybersecurity in International Arbitration (**C-5**)

reasonable measures are put in place to protect confidential data and that adequate data notices are posted on the websites of counsel, arbitrators, and the PCA to ensure reasonable compliance with the GDPR.

55. The Explanatory notes to the IBA-ICCA Roadmap consider this issue as follows:

> At the time data is collected from a data subject, the data subject must be provided with detailed information about the manner and means by which the data will be processed as described in the GDPR (Art. 13). Similar rights attach when the controller did not collect the data in the first place, which often is the case in international arbitration (Art. 14). For example, the law firm often will not have originally collected the personal data that a party supplies for use in an arbitration. The same is true of all Arbitral Participants (apart from the parties).
>
> Compliance with the transparency requirements of the GDPR obligates all the controllers of personal data to ensure that data subjects whose personal data may by processed as a part of an arbitration are provided with transparent information complying with Articles 12-14 of the GDPR.
>
> To ensure that data subjects are notified, the GDPR requires all data controllers, including those who receive data from sources other than the data subject, to provide notice. There are significant exceptions to this notice requirement to avoid overlapping notices and undue burden. However, each Arbitral Participant remains liable if proper notice is not provided to the data subject. The question is how to apply these principles to ensure that proper notice is provided but multiple notices are avoided. [33]

56. The Explanatory notes to the IBA-ICCA Roadmap makes specific comments on confidentiality that are directly relevant to this confidentiality order. The Task Force states:

> The Working Party has made clear that data subject rights to transparent information about the processing of his or her data, access to that data, and the right to rectify it, continue to apply to data when processed for litigation purposes. With respect to the access and notice requirements, the Working Party has said that:
>
> > [I]n the context of pre-trial discovery, [transparency] would require advance, general notice of the possibility of personal data being processed for litigation. Where the personal data is actually processed for litigation purposes, notice should be given of the identity of any recipients, the purposes of the processing, the categories of data concerned and the existence of their rights.

[33] Data Notices are discussed at IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 21 – what notification requirements apply. (**C-3**)

> Therefore, any justification for withholding such notice in the arbitration context would need to be something unique to arbitration, for example, confidentiality. However, the GDPR provides that confidentiality can only be a basis for not providing the requisite data privacy notice when the information was not obtained from the data subject and "*the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy*" (Art. 14(5)(d)). This standard will typically not be met by arbitral confidentiality generally, although it may apply to counsel who is subject to legal privilege and to the arbitrator's duty of confidentiality.
>
> In the context of an arbitration requiring specific data privacy notices informing all data subjects named in the evidence of the fact of the arbitration, where the personal data is being transferred, and who the arbitrators are (among other things), is not only a significant burden but may also effectively mean that the arbitration is no longer confidential. This is further complicated in sensitive cases when the provision of notice itself could be problematic. [34]

57. Accordingly, Data Notices and the potential for contractual clauses concerning data in existing documents and new documents are necessary considerations in a Confidentiality Order and should also be considered in the context of other procedural orders may by the Tribunal.[35]

58. For the reasons set out above, the Investor proposes that the Tribunal defer making a Confidentiality Order until after information has been produced by all participants in this arbitration first to facilitate the Data Privacy and Security issue.

III. Concerns not arising from Data Privacy

59. A particularly important factual issue is the confirmation of illegal despoliation of evidence by senior Ontario government officials. Such despoliation appears to affect relevant and material documents in this arbitration. In particular, senior officials in the Office of the Premier of Ontario were criminally convicted for the destruction of such electronic evidence. Trillium Power, a non-party to this arbitration, who sought a wind power energy contract under the same Ontario Feed-in Tariff has an ongoing case in the Canadian courts involving the destruction of such evidence relating to wind power contracts. The fact of the unlawful destruction has been canvased in the Claimant's Notice of Arbitration and by the Canadian courts in criminal convictions which occurred after the filing of the Notice of Arbitration. The illegal destruction of this important evidence has been widely reported in

[34] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 21 - what notification requirements apply. (**C-3**);

[35] IBA-ICCA RoadMap - Explanatory Notes at Explanatory Note 21 - what notification requirements apply. (**C-3**);

the Canadian media.[36]

60. Much of the wrongful conduct in this arbitration was directed from the Office of the Premier of Ontario. The destruction of such evidence is disconcerting. The *Toronto Star* reported on the conviction of David Livingston, former Chief of Staff to the Ontario Premier, as follows:

> "A former chief of staff to Dalton McGuinty is guilty of deleting documents in a "dishonest" scheme to protect the Liberals from the fallout of power plants axed before the 2011 election, a judge ruled Friday.
>
> ... The judge said both Livingston and Miller arranged for the "indiscriminate wiping" of the hard drives of 20 computers in the McGuinty premier's office before Kathleen Wynne took power in February 2013 — despite legal orders from a legislative committee to produce relevant documents on the controversial power plant cancellations."[37]

61. In such exceptional circumstances, it appears necessary for the Investor to obtain evidence from third persons who received the illegally destroyed emails. The Investor reasonably believes that relevant and necessary evidence exists with recipient companies in the United States. Such evidence can be obtained through recourse to American domestic law that assists the international arbitration process — namely, the Section 1782 process and procedures under the *Federal Arbitration Act* (FAA).

62. The illegalities have been widely reported in the Canadian media.[38] *Global News* reports that Trillium Wind Power has sought production of hard drives from the government that might still contain remnants of emails discussing wind power contracts under the Ontario FIT Program. It reported:

> "Trillium says documents related to their case were deliberately destroyed by senior government staff to "defeat or disrupt" its ability to prove its accusations in court. These actions, according to Trillium, amounted to the

---

[36] See Investor's Notice of Arbitration at paras. 87-88, 113-123, which relied on newspaper reports of the charges and subsequent criminal conviction of the most senior official in Ontario Premier Dalton McGuinty's office for arranging to have all electronic records of a number of computers in the Premier's offices illegally "wiped" by a cyber professional to ensure that all evidence of communications had been destroyed.

[37] Rob Ferguson, Toronto Star, January 19, 2018, "Former McGuinty chief of staff found guilty of deleting documents in wake of power plants cancellation" (**C-9**) https://www.thestar.com/news/queenspark/2018/01/19/former-mcguinty-chief-of-staff-david-livingston-found-guilty-of-deleting-documents-in-wake-of-power-plants-cancellation.html

[38] See Investor's Notice of Arbitration at paras. 87-88, 113-123, which relied on newspaper reports of the charges and subsequent criminal conviction of the most senior official in Ontario Premier Dalton McGuinty's office for arranging to have all electronic records of a number of computers in the Premier's offices illegally "wiped" by a cyber professional to ensure that all evidence of communications had been destroyed.

> "deliberate concealment of the evidence of misfeasance in public office," which is the claim the company has made against the government."[39]

63. The *Hamilton Spectator* newspaper reported:

> Trillium is now seeking court approval of a motion to force the government to search 52 computer hard drives from the McGuinty premier's office for any documents related to the offshore decision, which the company says was based more on "political science" than natural science, over fears offshore wind opponents would vote against the Liberals.
>
> ... Twenty-four of the 52 hard drives sought by Trillium were the subject of intense scrutiny and in last year's trial of two former key McGuinty aides over deleted documents in the cancellation of two gas-fired power plants, also before the 2011 election. Former chief of staff David Livingston was convicted and sentenced to four months in jail."[40]

64. The Investor understands that the disposition of these matters in the Ontario courts by this non-party is currently underway. The Investor is of the view that it is more probable that evidence can be obtained from persons located in the United States. Such persons successfully produced evidence in the Mesa Power Claim.

65. To this end, the Investor wishes the Confidentiality Order to confirm that in light of these extraordinary circumstances where evidence has been despoiled that leave has been granted pursuant to section 3(9) of the 2010 version of the IBA Rules to permit the Investor on its own to seek remedies from local courts to obtain evidence that would reasonably be expected to have been despoiled.

66. To make matters worse, counsel for the Investor wrote to the Deputy Attorney General of Canada as early as June 1, 2017, putting the Respondent on notice of its duty to protect relevant and material information in this case. On June 1, 2017, the Investor wrote to the Deputy Attorney General of Canada advising him to take steps to collect and preserve relevant and necessary evidence relating to this dispute. The Investor notified the Tribunal in an email of February 11, 2019, that it had written to Canada seeking confirmation that such preservation steps were taken and noted that the Investor had not received a response. The Investor has received no response to this day on this issue from Respondent.

---

[39] Brian Hill, Global News, April 30, 2018, "Trillium Power releases new evidence alleging Ontario Liberals destroyed documents during $500M lawsuit", (**C-10**), https://globalnews.ca/news/4175888/trillium-power-alleges-ontario-government-destroy-documents-lawsuit/

[40] Rob Ferguson and Robert Benzie, Hamilton Spectator, November 5, 2018, "Wind energy company accuses PC government of aiding Liberal 'cover up'" (**C-11**): https://www.thespec.com/news-story/9007880-wind-energy-company-accuses-pc-government-of-aiding-liberal-cover-up-/

67. As the record demonstrates, there was a significant role in the matters at issue in this arbitration played by officials in the Ontario Premier's Office. Thus, given such exceptional circumstances where it is likely that Respondent has improperly destroyed evidence, it is necessary for the Investor to obtain evidence from the recipient persons, who received the illegally destroyed emails.

68. The Investor reasonably believes that relevant and necessary evidence exists with recipient companies in the United States. Such evidence can be obtained through recourse to American domestic law that assists the international arbitration process — namely, the Section 1782 process and procedures under the *Federal Arbitration Act* (FAA). Indeed, the Investor in *Mesa Power Group v Canada* obtained evidence from US parties under the US Section 1782 process. The Section 1782 process allows a US District Court to assist a foreign or international tribunal in obtaining evidence from third parties to an arbitration. In the *Mesa Power Group* arbitration, key evidence from competitors for Ontario Feed-in Tariff energy contracts was located within the State of Florida, near New York City and close to San Francisco. The competitors of Mesa Power Group seeking Ontario Feed-in Tariff Contracts would also be competitors of Tennant Energy.

69. Confidentiality is a fundamental part of the arbitration process. This need for confidentiality needs to be thoughtfully and properly balanced carefully with the public interest in disclosure. Without the protection of confidential business documents from public disclosure, there would be a serious impediment against adducing sensitive information for the consideration by an arbitral panel.

70. Given the likelihood of receiving information obtained from local courts, and subject to court confidentiality orders, special consideration also needs to be given to the protection of information obtained from third parties. The confidentiality of such designated documents should be respected in the NAFTA process through any Confidentiality Order issued by the Tribunal. Canada's proposed order does not address this matter.

71. The issue of how to treat the assertion of confidentiality by domestic courts resulted in ongoing procedural difficulty in the Mesa Power Group NAFTA Claim.

72. Simply put, where confidentiality has been asserted over these documents by third parties involved or by a court, such designation needs to be recognized and protected. This confidential nature of the evidence does not prevent the court or the disputing parties from reviewing the information, and it merely has an impact on public disclosure.

73. The Tribunal and Canada would always receive fully unredacted copies of these confidential materials. As a matter of both principle and practicality, all that issue is Canada' s desire to make the unredacted documents public, in violation of those Court orders.

74. The *Mesa Power* Tribunal, under the terms of the Confidentiality Order, ordered the declassification of thousands of pages of evidence obtained in the US domestic court process. That Tribunal ruled that the evidence obtained by Third Parties did not meet the

technical requirements for confidentiality under the Tribunal Order even though they met the requirements of protected confidential information under the binding terms of domestic court orders. As a result, the Investor, Mesa Power, was obliged to review and redact significant amounts of information to comply with the Tribunal's order.

75. Furthermore, the Tribunal and disputing parties had to undergo contested procedures to address whether the information protected by the court orders met the technical requirement for confidentiality under the Tribunal order.

76. Mesa Power Group was compelled to redact thousands of pages of evidence to facilitate public disclosure under the terms of the Confidentiality Order, and subsequent rulings, by the Mesa Power Group NAFTA Tribunal.

77. Canada has advocated for a Confidentiality Order in the current case like the burdensome and wasteful wording used in *Mesa Power* that would compel the Investor to provide redacted "declassified" versions of all evidence and all documents used in the arbitration. Producing the declassified documents is very laborious and imposes great expense to the Investor. Furthermore, the orders advanced by Canada have artificially short periods to produce declassified documents that increase the cost and hardship to the parties. For the unfairness and burden, Canada's proposals must be rejected.

78. In the *Mesa Power Group* case alone, the Investor had to incur many hundreds of thousands of dollars of cost to comply with these obligations, and there were numerous motions on the sufficiency of the redaction.[41] Even more astonishing was the recent discovery by counsel for the Investor that none of the declassified materials filed in the *Mesa Power Group* or *Windstream* claims were made available to the public. Despite Canada's claims to support transparency, there was no public transparency at all concerning this evidence.

79. After this discovery, Counsel for the Investor wrote to counsel for the Respondent on February 20, 2019, and again on February 26, 2019,[42] enquiring about the status and the production of evidence that had been produced in the *Mesa Power* and *Windstream Power* NAFTA Claims. Production of non-confidential evidence filed in these two NAFTA claims, if produced in the current case, could substantially reduce the need for some, but not all, of the document requests that might need to be made to US courts.

80. The Investor's February 26th email stated:

> We noted in our February 20th email that non-confidential evidence was filed in the two NAFTA arbitrations about Ontario's Feed-in Tariff involving Canada,

[41] A similar obligation was not required in the *Windstream* case as such evidence from domestic courts was not part of the record.

[42] Email – Barry Appleton to Lori Di Pierdomenico February 26, 2019 (also setting out the text of the February 20, 2019 email from Barry Appleton to Respondent seeking declassified materials filed in the Mesa Power and Windstream NAFTA Claims). (**C-7**)

> namely Windstream and Mesa Power. We noted that we looked at Canada's NAFTA website and the PCA website for each of these NAFTA cases. We have not been able to locate public access to the declassified evidence available for either case on Canada's website or at the PCA.
>
> We note that you have refused to respond to our request about the location of the documents, just as you have refused to address other procedural questions, we have posed to you about the preservation of documents or the filing of a Statement of Defense. To be clear, our enquiry to you right now is about the current public availability of this declassified public information.[43]

81. In a response on February 27, 2019, Canada confirmed possession of the non-confidential materials, and that none of this information had been made public. The email stated:

> While the exhibits in the Mesa and Windstream arbitrations are not posted on the PCA website, this information may be subject to public disclosure in accordance with Canada's domestic laws.[44]

82. The Confidentiality Order proposed by Canada has the effect of causing hardship to the Investor which is not equally borne by the Respondent because the Respondent has unlawfully destroyed evidence. Since the declassified information has not been made public by Canada, there has been no benefit associated with the activity for the Investor, only a significant burden imposed upon the Investor. Not only is the effect disproportionate to the benefits, but the costs have not been carried equally – but have been disproportionately carried by the Investor. Such a situation should be permitted to occur.

83. Furthermore, in light of Canada's admission that it has such non-confidential information available, Canada should immediately disclose the extent and content of such information, and further to the requests made by the Investor in June 2017, finally confirm whether it has taken steps to protect and preserve such essential information.

84. Based on the preceding, Canada's suggested approach set out in its draft Confidentiality Order should not to be followed. Canada approach is inconsistent with the Tribunal's obligations under NAFTA Article 1115, and Article 15 of the 1976 UNCITRAL Arbitration Rules.

---

[43] Email – Barry Appleton to Lori Di Pierdomenico, February 26, 2019 (also setting out the text of the February 20, 2019 email from Barry Appleton to Respondent seeking declassified materials filed in the Mesa Power and Windstream NAFTA Claims). (**C-7**)

[44] Email – Lori Di Pierdomenico to Barry Appleton, February 27, 2019 (**C-8**)

IV. Concerns not arising from Data Privacy

85. For the reasons set out above, the Investor that the Tribunal:

a. Obtain information necessary to make determinations concerning coverage and lawful transfer of data under the GDPR;
b. Defer making a Confidentiality Order until after such information in paragraph a has been produced;
c. Issue a procedural order addressing data privacy and security obligations in this arbitration; and
d. Provide an opportunity for the disputing parties to develop a confidentiality order subsequently.

All of which is respectfully submitted.

Submitted this 23rd day of April 2019 on behalf of counsel for the Investor.

_____

Barry Appleton

Appleton & Associates International Lawyers LP
77 Bloor St. West, Suite 1800
Toronto, ON M5S 1M2

Reed Smith LLP,
1001 Brickell Bay Dr, Suite 900
Miami, Fl 33131

Counsel for the Investor