Office of the Privacy Commissioner of Canada
30, Victoria Street
Gatineau, Quebec
K1A 1H3

BY E-MAIL: OPC-CPVPconsult2@priv.gc.ca

Montreal, August 6th, 2019

Dear Sir or Madam,

Subject: Consultation on transfers for processing data – Reframed discussion document

We would like to thank the Office of Privacy Commissioner of Canada for the opportunity to participate in this consultation regarding cross border data transfers.

A. Introduction

(i) The Digital Age and Participation in the Information Society: The role of blockchain technology in the digital revolution[i]

Data is knowledge. Knowledge is power. Today, data is constantly flowing from one device to another based on a series of rules and thresholds set by technology developers and manufacturers and executed by mathematical algorithms. The data that consumers and users are required to provide to access products and services (commonly referred to as Apps) that they want to use to partake in the digital wold are *quasi* non-negotiable – users must agree or be denied service.[ii] The narrative created by companies building, selling and/or offering these tools (or Apps), that consumers have a choice not to use their products, is also less and less true as few companies maintain global market control over widely used online tools and apps.

In fairness to the current marketplace, the data revolution thus far has demanded companies focus on gathering as much data as possible to gain competitive business advantages to meet the marketplace demands for intelligent and "aggregate data", "metrics" and the like. For users, the access to the proliferation of "free" services has also been transformational. More people are online, using mobile devices, and connecting to the global digital economy. As this transformation has been occurring, the world population has experienced a true global industrial revolution that shows no signs of stopping.

Of late, civil society and governments have been pushing back on the *status quo* surrounding data control and flows. It is increasingly clear that there must be reconsideration of the balance of data captured to access (through online services designed by corporations) the global digital society and economy with the ability to control one's own identity.[iii] We have hit a tipping point. Arguably, the tipping point came in 2008-09 with the global recession most visibly, but in a quieter and more pervasive way, it can also be seen in relation to the emergence of blockchain and demand for self-sovereign digital identity.

While foreign governments have adopted different approaches to address digital privacy issues and have enacted new laws (or amended existing legislation) to establish data protection frameworks,[iv] technology has simultaneously evolved to respond to citizens' preferences to manage their own individual digital identities (i.e., identity management) through the use and adoption of blockchain technology for identity management.[v]

Rather than risking any exposure (i.e., data breaches, footprints, *etc.*), blockchain technology can achieve a number of important outcomes, including: (i) enable real-time access to ownership information,[vi] (ii) facilitate digital consent management[vii] (consisting of a process that allows a website to meet legal requirements by obtaining user consent for collecting their data through cookies during their visit).[viii] In addition, while some postulate how important blockchain will be for the world economy[ix], others raise issues of data governance and "[…] lack of standards and frameworks to govern the integrity, security and application of such data"[x], amongst other concerns.

Our digital connectivity feeds into the digital economy[xi] and the issue of how consent is given by the end-user (i.e., the consumer) must be exhausted, both in form (i.e., with possible use of blockchain technology) and substance.[xii]

Trans-border data flows impact domestic and global privacy regulatory and business frameworks. In Canada, the national privacy dialogue is largely driven by the OPC, as a mandated agent of Parliament to oversee "[…] compliance with both the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), Canada's federal private-sector privacy law."[xiii] As such, it is respectfully submitted that any national initiatives relating to the protection and promotion of Canadian's privacy framework should be led by the OPC who should coordinate accordingly with interested and relevant departments or agencies.[xiv] Globally, the manner in which Canada extends its privacy frameworks to apply to the digital economy requires close collaboration between the OPC, Global Affairs and other relevant departments or agencies dedicated to global trade and global issues pertaining to Canadians. As such, we believe it is imperative that the OPC advance its understanding and expertise on blockchain technology for the purpose of navigating its evolving role domestically with the public and private sectors who are innovating in the space, as well as for the purpose of informing the Government of Canada on global issues impacting Canadians.

(ii) Individual versus enterprise data

Another factor that must be considered within the context of this consultation is the difference between user data (i.e., a person's data, or data subject) and enterprise data[xv], which is usually processed by suppliers for the purpose of enterprise data analytics[xvi] (and benchmarking). The performance of these services are predicated to Master Services Agreement ("MSAs"), Software as a service Agreement ("SaaS")[xvii], Terms and Conditions ("T's and C's") and/or Terms of Use ("ToU"), in which the co-contracting Parties have most likely considered the following contractual terms, such as: (a) licenses to customer and third party data (i.e., employer and enterprise data) as to perform the services (i.e., processing enterprise data), (b) respecting privacy law and customer policies (with respect to data safeguards, data retention and information security policies, keeping enterprise data segregated, physically or logically, from the information of any other third party, etc.).

Of note, consent in the enterprise context poses certain issues worth further reflection.[xviii] For example, under GDPR, employers cannot hold their employee's data without their consent, which can be withdrawn at any time. The UK Information Commissioner has issued guidance with respect to the degree of consent required in employer-employee relationship.[xix] Though the situation in Canada is more opaque, it should be clearly indicated by the OPC that the procurement of consent should be borne by the data collector (at the initial point of collection, primarily by the employer, or 'data controller') and not *downstream*, by the data processor. To create obligations on the data processors would be very onerous, both on an operational and technological levels.

(iii) GDPR and Adequacy Decisions

In May 2018, the European Commission released the General Data Protection Regulation (EU 2016/679),[xx] which:

- "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data" (at paragraph 1);

- "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (at paragraph 2); and

- stipulates "[t]he free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."

In order to permit cross-border data flows to countries outside of the European Union without any further safeguard being necessary, the designated country must benefit of an Adequacy decision.[xxi] Co-contracting parties to the agreement will also execute standard contractual clauses, as will be discussed below. In comparison to *PIPEDA*, the GDPR creates more obligations onto data controllers and processors, including: (i) approaches to consent as a legal basis for data processing, (ii) a right to data portability, (iii) a right to be forgotten (or erasure), (iv) data breach reporting, and (v) approaches to processing employee data.[xxii] It is also worth noting that Canadian businesses have already been subject to enforcement actions under the GDPR.[xxiii] In this regard, what should be of concern to the OPC is that if the European Commission revokes Canada's adequacy status, it would create a substantial amount of turmoil for Canadian businesses who process data emanating from the European Union, especially considering the ratification of CETA. Further consideration would also have to be afforded to the EU's e-privacy Regulation ("ePR")[xxiv], which would complement the GDPR on the electronic communications data that qualify as personal data, such as the requirements for consent to the use of cookies and opt-outs.

In this regard, it is respectfully submitted that the OPC must take the lead in providing a novel framework that enables Canada to play a role leading global data governance standards while amplifying and promoting frameworks and technologies that are future forward, such as those emerging that leverage blockchain technology solutions.

(iv) Why this consultation is so important and why it must be acted upon?

As a result of the foregoing, Canada has the opportunity to take advantage of its global position, innovation resources, political stability, and leading work on privacy frameworks to not only adhere to its international commitments,[xxv] but be at the forefront of global privacy law and promote innovation in the rapidly emerging blockchain ecosystem.[xxvi]

Considering, (i) competing interests of various stakeholders (including federal ministries), (ii) recent data breaches, and, (iii) Canada's unique position, politically, geographically, climatically, access to natural resources (access to energy), technology hub (AI, mining, etc.), it is respectfully submitted that Canada owes it to itself to foster privacy aligned participation of its citizens and industry in the digital era. The Canadian privacy narrative and framework should be reviewed to ensure that it promotes a robust global privacy framework, aligned to other critical economic policy objectives, including the promotion of innovation (including blockchain) in the data/IT world, cybersecurity and national security, technology neutrality,[xxvii] and cross-sectoral growth overall.

<u>General Recommendations</u>

1. Create and mandate an industry and cross-departmental Task Force to work with innovation leaders to understand the applicability of blockchain technology in the context of privacy and trans-border data flows;

2. Where this has not been done, the OPC should align Canada's privacy laws with those of the GDPR so as to: (a) increase global competitiveness, (b) maintain adequacy decision, (c)

respect trade-agreements with particular regard to Canada-EU Comprehensive Economic Trade Agreement and other existing agreements and negotiations;[xxviii] and,

3. Review and update Canada's privacy narrative and framework to ensure that it promotes a robust global privacy framework, aligned to other critical economic policy objectives, including the promotion of innovation (including blockchain) in the data/IT world, cybersecurity and national security, technology neutrality,[xxix] and cross-sectoral growth overall can be achieved.

Responses to Questions

In general, it is unclear what new problems this consultation is addressing or what new reason there is that would provide a justification to consider new legislation at this time. Most recently, the Digital Privacy Act was introduced in Canada following significant consultation with industry. It is our view that it is too soon to determine if this legislation has in fact left gaps that require additional measures. As such we support the recommendations we have provided above. Below are more specific considerations aiming to help the OPC as it works through this consultation process.

1. How should a future law effectively protect privacy in the context of trans-border data flows and transfers for processing?

This is a critical question that requires additional consideration with industry as well as a review relating to the treatment of cross-border data flows under public and private international law. It would be very difficult for the OPC to extend its jurisdiction beyond Canadian borders. Protecting Canadians in Canada and addressing uses of data that occur in Canada or transit through Canada should be the area of focus of the OPC going forward. An international data agreement may serve to clarify items regarding trans-border data flows.

Moreover, a new law may not be the most effective instrument to protect privacy in the context of trans-border data flows. Technology, such as blockchain technology, offers a more rapid protocol to encrypt and secure data and an individual's private information. The Government of Canada has been working for a number of years to design updated technology systems and protocol to enhance security in this regard.[xxx]

In the short term, it is reasonable to expect, and enforce, existing legal and contractual obligations, namely:

(i) Compliance to applicable privacy laws, both where the data is collected (i.e., Europe) and where it is processed (i.e., Canada), including for example, Adequacy decisions, EC Standard contractual clauses[xxxi], as well as ensure organization compliance to these laws;

(ii) Compliance to contractual representations and warranties, in which the data subject provides his or hers consent and authorizations to the transfer of their data to the co-contracting party for purposes of processing in another jurisdiction;

(iii) The contract should indicate where the servers are geographically located; thereby addressing the distinct notions of data sovereignty, data residency and data localization;[xxxii]

(iv) Adherence to information security protocols and security questionnaires (i.e., risk assessment questionnaires as completed by data processors)

(v) Adherence to organizational protocols – internal review processes & toolkits.

2. **Is it sufficient to rely on contractual or other means, developed by organizations and reviewed only upon complaint to the OPC, to provide a comparable level of protection? Or should a future law require demonstrable accountability and give a public authority, such as the OPC, additional powers to approve standard contractual clauses before they are implemented and, once they are adopted, proactively review their implementation to ensure a comparable level of protection?**

At this time, there is no clear rationale or use case that demonstrates that the OPC requires additional powers, not least given that new powers and enforcement measures have recently come into force. In the meantime, it would be sufficient to rely on contractual means. That said, subjecting contractual approval to the OPC would be detrimental to the efforts of co-contracting parties for numerous reasons, including:

(i) Would render the negotiation and closing of contracts nearly impossible (further creating significant delays);

(ii) Go against the contractual 'intent of the Parties' as well as principles of contractual interpretation;[xxxiii] and,

(iii) Could create obligations on Parties that are too onerous, with particular regard to liabilities. By way of example, reference can be made to Clause 5 and 6(2) of the EC-SCC (to non-EU countries).[xxxiv]

Indeed, those who are receiving data from foreign countries should have already conducted a certain level of due diligence (i.e., information security checklists, risk assessment questionnaires, etc.) to be able to provide comparable levels of protection. In addition, it should be incumbent on the original source of data (data controller) to ensure that it is allowed to transfer data to another country for purposes of processing and respect its contractual obligations to its clients. In other words, most contracts oblige data processors to be located within particular jurisdictions.

3. **How should a future law effectively protect privacy where contractual measures are unable to provide that protection?**

Such a speculative question is difficult to address in detail without the provision of clear context or a discussion of additional concerns. The more effective way forward would be to ensure that an industry advisory task force is established to keep the OPC abreast of emerging technology and data trends that may result in new information or context justifying further OPC oversight or legislative response.

4. **In your view, does the principle of consent apply to the transfer of personal information to a third party for processing, including trans-border transfers? If not, why is the reasoning outlined above incorrect?**

In order to be able to transfer personal information to a third party for processing, the data controller (i.e., the initial collector of data) should be have received consent from the data subject in order to transmit such data to a third-party processor. This must be obtained by way of consent, namely through contract (or employment agreement for enterprise/employer data) or other form of recorded authorization, as stated in this document, as well our response to question #6, most preferably with the use of blockchain technology.

5. **Does Principle 4.1.3 affect the interpretation or scope of the principle of consent? If so, what is the legal basis or grounds for this interpretation?**

Principle 4.1.3 states that:

an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third-party for processing. Organizations must use contractual or other means to provide a comparable level of protection while the information is being processed by a third-party.

In giving the words of this Principle a 'natural and ordinary meaning', any organization that possesses or has custody of personal information would be *responsible* for it. Not only is this word broad, but as mentioned in this document, it is opined that it the initial data collectors responsibility (and obligation) to obtain consent from the data subject and set out the grounds (or legal basis). To demand subsequent processors of data to obtain further consents (and/or verify said consent) from the data subject would be onerous thereon. Issues of consent are provided for in other sections of *PIPEDA,* including for example sections 6 and 7, as well as clause 4.3 of Schedule 1, amongst others.

6. What should be the scope of the consent requirements in the Act in light of the objective of Part 1 of PIPEDA as set out in section 3, the new section 6.1 (and its reference to the nature, purpose and consequences of a disclosure), and the OPC's Guidelines for obtaining meaningful consent, in force since January 1 2019?

Specifically:

a. In what circumstances should consent be implicit or explicit?

In general, the OPC has been advised by industry regarding consent through the consultations that immediately preceded the introduction of the Digital Privacy Act. There has been no immediate or obvious change in the commercial context that would suggest additional consultation regarding consent is required at this time. However, as is always good to recall, consent is that it is not static to the initial point of information collection. Companies are required to advise consumers and users when their terms of service and offerings change. Standards for consent should be aligned in the same manner as they are at initial collection. In practice, informed consent should be verified as the purpose of use of PII data changes. Consent can also be withdrawn at any time and companies should make such a withdrawal obvious and easy for users.

Consent should be informed and explicit and should be recorded by technological means, including use of blockchain technology so as to determine consent in an immutable "point in time" record.

b. What should be the level of detail in the information given to the person affected? Do you agree that consent should be comprised of at least the following elements: (i) the purposes for which the responsible organization seeks to use the personal information, (ii) the fact that it uses third parties for processing but that it provides for a comparable degree of protection, (iii) when the third parties are outside of Canada, the countries where the personal information will be sent, (iv) the risk that the courts, law enforcement and national security authorities in those countries may access the personal information?

Yes with respect to items (i) to (iii), excluding (iv) and wherein one would have to accept the application of foreign sovereignty, data sovereignty, unless the 'defendant' raises a comparable common law - *forum non conveniens* (or conflict of laws) or equivalent legal objection. Alternatively, export control regulations (equivalent to the U.S.) could be adopted or added for contractual purposes. We encourage the OPC to consult internally with the Department of Justice and other relevant departments regarding its enforcement mandate and capacity for such requirements, not least item (iv). As industry stakeholders, it is recommended that a proposal be drafted by the OPC and shared for further consultation as further context and specificity are fundamentally important to provide an informed answer to this question.

c. Should the notice to the affected person name the third parties?

Ideally yes, but, realistically, blockchain technology would be required to establish 'chain of title' (or use) of data to know who had access to a person's PII.

d. Should the notice contain other pieces of information?

Idem.

7. Since the 2009 Guidelines already require that consumers be informed of trans-border transfers of personal information, and of the risk that local authorities will have access to information (preferably at the time it is collected), at a practical level, would elevating these elements to a legal requirement for meaningful consent significantly impact organizations? If so, how?

No response.

8. If the elements identified in question 6(b) were required conditions for meaningful consent under a new OPC statement of principle, what steps should the OPC take to address the needs of organizations to collect, use, and disclose personal information?

Please refer to answer provided in 6(b). It is unclear what is intended as a consequence for failure to comply with "a new OPC statement of principle". As industry stakeholders, it is recommended that a proposal be drafted by the OPC and shared for further consultation as further context and specificity are fundamentally important to provide an informed answer to this question.

9. What elements should be included in obtaining consent for transfers for processing that are not trans-border?

One of the only useful elements to ensure procurement of consents are (1) the technological means in which consent is obtained and recorded same, (2) the satisfaction of the requirements of consent, including:

1. Verification of the identity of the subject who will be electronically signing an eIC (i.e., KYC);

2. Present the eIC in an understandable manner (i.e., what are the contents of the eIC?);

3. Record the eIC, from the first date of consent; hence an excellent use case of blockchain for consent management[xxxv] (or "chain of title");

4. The eIC must be secure with restricted access and should include methods to ensure confidentiality regarding the subject's identity, participation, and personal information after informed consent has been obtained;

5. The subject's information within an electronic system must be encrypted, unless the entity documents why encryption is not reasonable and appropriate in their specific circumstances and implements a reasonable and appropriate equivalent measure.

The technological means must be able to continuously be able to capture each of the foregoing elements, per jurisdiction of data subject, type of data, electronic informed consent, etc.[xxxvi]

10. Do you think the proposed interpretation of PIPEDA is consistent with Canada's obligations under its international trade agreements? If not, why would the result be

different from the current situation, where the elements identified in question 6(b) must disclosed as part of the openness principle?

As a result of its abundance of clear and renewable energy, security, technology, amongst other reasons, Canada is well placed to: (i) set international standards in privacy matters and compliance, and (ii) attract technology driven companies and data centres[xxxvii] for collecting, storing and processing data, including big data analytics[xxxviii] (if done on a non PII, deanonymized, aggregate manner).

11. Any other comments or feedback you think may be helpful.

Not at this time.

We hope that these comments are useful for the OPC and should you have any further questions, please do not hesitate to contact the undersigned.

David Durand
Durand Morisseau LLP
ddurand@durandmorisseau.com

Tanya Woods
canada@digitalchamber.org

References

[i] See: https://www.springer.com/gp/book/9789462391826; See also: https://s3.amazonaws.com/academia.edu.documents/48780763/MIT_Digital_Technology.pdf?response-content-disposition=inline%3B%20filename%3DEmbracing_Digital_Technology_A_New_Strat.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190623%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190623T111445Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=662f9b5fd1a60ee47380595a38dbc8e7270c3101d9d49f5efa0a14fd8d62f170; and https://www.mckinsey.com/business-functions/organization/our-insights/unlocking-success-in-digital-transformations; other good publications on digital transformation.

[ii] In this regard, our data, including personal information or personal identifiable information ("PII"), enables us to (i) sign-in into our various online accounts (which can be located anywhere in the World), (ii) engage in financial transactions (involving financial information, for purposes of online banking and payments, dealing in virtual currencies (also known as crypto-assets or digital assets), open banking (and application programming interfaces, API's), (iii) circumvent traffic (i.e., with mapping and traffic algorithms), (iv) communicate with others via social networks, and, (v) run our devices on the IoT (including our smart home systems, health monitoring devices, and entertainment systems, *etc.*), amongst many other practical uses. To partake in the global digital world that has emerged and is empowered by our data every day, consumers and users must agree with to the myriad of end user agreements, privacy policies, use of cookies and so on otherwise providers/suppliers, individuals (users or data subjects) have little to no access to the platforms and products they are expected to use or have in today's digital society. Further, while there is a right in some parts of the world to erase one's digital footprint and go off-grid, in reality it cannot be done without: (i) affecting platform functionality (and inherently "quality of life"), (ii) stifling innovation, or becoming invisible and excluded from the rest of the world. The result is hardly democratizing. Where centralized control systems are in place, for example, where one entity sells all of the products that a person can interface with and consumers and participants in the digital economy never really have full control over their data, identity, or privacy – let alone control regarding what happens with their information across borders.

[iii] See: https://www.nytimes.com/2019/07/16/technology/big-tech-antitrust-hearing.html, https://www.priv.gc.ca/en/opc-news/speeches/2019/s-d_190805/

[iv] Including analogous anti-spam frameworks, such as CASL: https://www.fightspam.gc.ca/eic/site/030.nsf/eng/home and Canada's *Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act* (S.C. 2010, c. 23), available at: https://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html.

[v] See for example the contents of U.S. Pat. No. 9,772,790 B2, issued on August 1st, 2017 (available at: https://patentimages.storage.googleapis.com/b0/6f/51/e507abe3895947/US9722790.pdf), as well as U.S. Pat. No. 9,635,000 B1, issued on April 25th, 2017 (available at: https://patentimages.storage.googleapis.com/84/03/e0/5611dfd48e898f/US9635000.pdf).

[vi] See: https://www.forbes.com/sites/forbesrealestatecouncil/2018/06/22/will-the-power-of-blockchain-mean-the-end-of-title-insurance-companies-in-20-years/#3dd2e450342a

[vii] See: https://worldwide.espacenet.com/publicationDetails/biblio?II=2&ND=3&adjacent=true&locale=en_EP&FT=D&date=20190103&CC=US&NR=2019005210A1&KC=A1; https://worldwide.espacenet.com/publicationDetails/biblio?II=13&ND=3&adjacent=true&locale=en_EP&FT=D&date=20130110&CC=US&NR=2013014278A1&KC=A1; and https://www.abe-eba.eu/media/azure/production/1979/eba_2018_obwg_b2b_data_sharing.pdf; Rantos, K., Drosatos, G., Demertzis, K., Ilioudis, C. and Papanikolaou, Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem.In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT, pages 572-577, available at: https://www.researchgate.net/publication/327658732_Blockchain-based_Consents_Management_for_Personal_Data_Processing_in_the_IoT_Ecosystem

[viii] See:https://www.researchgate.net/publication/330028734_The_Advantages_and_Disadvantages_of_the_Blockchain_Technology

[ix] See: https://www.bbc.com/news/business-48526666

[x] See: https://www.cpacanada.ca/en/news/innovation/2019-06-28-blockchain-data-governance

[xi] See: https://www.bankofcanada.ca/wp-content/uploads/2017/05/boc-review-spring17-dsouza.pdf https://www.bbc.com/news/business-48566024 and https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html

[xii] See: https://medium.com/@trbouma/game-plan-digital-identity-for-2019-7d602d1ba8b9

[xiii] See: https://www.priv.gc.ca/en/about-the-opc/what-we-do/mm/

[xiv] Both the Minister of Innovation, Science and Economic Development Canada's ("ISED") and the Competition Bureau have waded into Canada's privacy framework in a manner that appears to be uncoordinated with the OPC. ISED has been actively promoting its Digital Charter: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html. The Digital Charter was conceived through ISED's National Digital and Data Consultations (launched June 19, 2018) entitled "*Canada's Digital Charter in Action: A Plan by Canadians, for Canadians*"[xiv], which is not without controversy. See: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html#s1 and, https://www.theglobeandmail.com/business/commentary/article-canadas-digital-charter-represents-a-sea-change-in-privacy-law-but/; https://www.theglobeandmail.com/business/commentary/article-five-reasons-canadas-digital-charter-will-be-a-bust-before-it-even/. Further, Competition Bureau Commissioner Matthew Boswell stated in an interview with *Canadian Lawyer* (published on July 2nd, 2019) that his "[…] vision for the organization is tied to the digital economy and the data-driven economy, to be a world-leading enforcement agency in terms of competition issues in the digital economy". See: https://canadianlawyermag.com/author/elizabeth-thompson/bringing-competition-to-the-digital-age-17393/; https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04464.html; and, https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201718/ar_201718/. It is worth mentioning that the notion of digital economy has also been adopted by the OPC.

[xv] Enterprise data comprises of: (i) corporate data (i.e., cost centres, operations, etc.), (ii) HR feeds (containing employee data and personal information), and (iii) third-party data (i.e., data the enterprise collects from its suppliers and centralized at the enterprise); and, https://www.techopedia.com/definition/28048/enterprise-data;

[xvi] See: https://open.alberta.ca/dataset/32e10a62-502d-48bd-bf81-e271e3c9d974/resource/732f3df7-2ab3-41e9-a9b1-a5e6ab4e02b2/download/goa-enterprise-data-analytics-strategic-planv1.0.pdf

[xvii] See: https://www.cio.com/article/3264013/saas-matters-key-caveats-for-saas-contracting.html

[xviii] See: https://www.forbes.com/sites/ashikahmed/2018/05/02/employee-data-privacy-in-the-gdpr-era-what-you-should-know/#51717bbd5c5c.

[xix] See: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

[xx] See: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679.

[xxi] See: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0002&from=en.

[xxii] See: https://iapp.org/news/a/matchup-canadas-pipeda-and-the-gdpr/

[xxiii]See: https://privatech.ca/2018/10/03/canadian-company-receives-first-gdpr-enforcement-decision/. See also: http://www.fcpablog.com/blog/2019/5/14/gdpr-enforcement-report-may-2019.html.

[xxiv] See: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

[xxv] See: https://www.eff.org/issues/tpp; https://www.washingtonpost.com/news/global-opinions/wp/2018/10/03/how-the-usmca-falls-short-on-digital-trade-data-protection-and-privacy/?noredirect=on&utm_term=.652387d3d3d6

[xxvi] For example, For example, consider our role in renewable and sustainable energy (https://mern.gouv.qc.ca/english/energy/index.jsp) (or power supplies) for data centres (https://www.hydroquebec.com/data-center/about.html) and data processing; climate change as referred to in the UN's – IPCC (https://www.ipcc.ch/) and Canada's position (https://www.canada.ca/en/services/environment/weather/climatechange/canada-international-action.html) with respect to this global issue; Canada's domestic and international policies, wherein Canada ranks within the top 10 safest countries in the World, Cybersecurity (http://worldpopulationreview.com/countries/safest-countries-in-the-world/). See also: National Cyber Security Strategy - Canada's Vision for Security and Prosperity in the Digital Age, available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx; https://www.itworldcanada.com/article/canada-is-a-prime-target-for-cybersecurity-attacks-in-2019/414201

[xxvii] Maxwell, Winston and Bourreau, Marc, Technology Neutrality in Internet, Telecoms and Data Protection Regulation (November 23, 2014). Computer and Telecommunications L. Rev. (2014), Forthcoming. Available at SSRN: https://ssrn.com/abstract=2529680 or http://dx.doi.org/10.2139/ssrn.2529680;

[xxviii] See: https://www.international.gc.ca/gac-amc/campaign-campagne/ceta-aecg/index.aspx?lang=eng ; https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/index.aspx?lang=eng, and Article 16.4 – Trust and confidence in electronic commerce stipulates: "Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards of data protection of relevant international organisations of which both Parties are a member."

[xxix] Maxwell, Winston and Bourreau, Marc, Technology Neutrality in Internet, Telecoms and Data Protection Regulation (November 23, 2014). Computer and Telecommunications L. Rev. (2014), Forthcoming. Available at SSRN: https://ssrn.com/abstract=2529680 or http://dx.doi.org/10.2139/ssrn.2529680;

[xxx] See: Pan Canadian Trust Framework, https://canada-ca.github.io/PCTF-CCP/?source=post_page----------

[xxxi] See: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en; See also: https://www.insightsforprofessionals.com/blog/data-sovereignty-vs-data-residency-vs-data-localization

[xxxii] See: https://www.insightsforprofessionals.com/blog/data-sovereignty-vs-data-residency-vs-data-localization

[xxxiii] *Sabean* v. *Portage LaPrairie Mutual Insurance Company* (2017 SCC 7), available at: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16361/index.do and further commentary thereon is available at: https://www.osler.com/en/resources/regulations/2017/defining-industry-specific-contractual-terms-supr.
[xxxiv] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=en
[xxxv] See: https://hackernoon.com/beyond-consent-blockchain-can-actually-ensure-data-privacy-3e7263e56cee; Genestier P, et al.,J Int Soc Telemed eHealth2017;5(GKR):e24, at: https://journals.ukzn.ac.za/index.php/JISfTeH/article/view/269 ; https://www.scitepress.org/papers/2018/69110/69110.pdf; and https://scholarspace.manoa.hawaii.edu/bitstream/10125/60121/1/0681.pdf
[xxxvi] See: https://www.hhs.gov/ohrp/regulations-and-policy/guidance/use-electronic-informed-consent-questions-and-answers/index.html. According to this guidance, electronic informed consent refers to the use of electronic systems and processes that may employ multiple electronic media, including text, graphics, audio, video, podcasts, passive and interactive Web sites, biological recognition devices, and card readers, to convey information related to the study and to obtain and document informed consent. See also: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_07_consent/
[xxxvii] See: https://www.theglobeandmail.com/report-on-business/economy/canada-competes/why-cold-canada-is-becoming-a-hot-spot-for-data-centres/article6598555/
[xxxviii] See: https://www.cigionline.org/articles/big-data-canadian-opportunity; https://www.ic.gc.ca/eic/site/101.nsf/eng/00012.html