Questions 1. Are there specific amendments needed to harmonize PIPA with other jurisdictions to make it easier for businesses to operate in all jurisdictions? **Continue reading for my answers to your questions are in bold. Thank you for letting People take part in this.**JOCr JOC*i* PP*i JK*

2. Are there specific amendments to PIPA needed to modernize the Act for relevant businesses and organizations to conduct business in Alberta? **Yes**

3. Question Should PIPA include a framework to regulate the design, development, and/or use of artificial intelligence systems within Alberta? If so, what should be included? **Yes, Cyber Policing and make it harder for companies to get person's information for I got Indentity Theft happen to me via my cell phone and they knew I had a bank account on my cell phone, now I removed that from my cell phone. Seniors are also vulnerable like children are.**

4. Questions: 1. Should all non-profit organizations be fully subject to PIPA for all their activities? 2. Should PIPA apply to political parties? **Yes even the constitutional levels need to answer to all levels and obey for they are the lowest level of all.**

Questions: page 14

5. Should provisions be added to PIPA to further protect potentially sensitive information? If so, for which information? **Harder to get personal information**

6. Should provisions be added for biometric information? **Yes, and have Cyber Policing too hopefully that will also help**

7. Should provisions be added to enhance the protection of children's personal information? **Why not include all individuals for all ages are being attacked.**

Page 16 8. Questions: 1. Are the provisions in PIPA dealing with forms of consent and the conditions attached to their use appropriate?

2. Should individuals receive notice in plain language when organizations explain the purposes for which personal information is collected, used or disclosed? **Yes and obey the laws and the consequences for not obeying the laws that are put in place.**

Page 18 Questions: 1. Should PIPA include other protections for individual information, such as an individual's right to be forgotten or de-indexed? **Yes**

2. Upon an individual's request, should organizations be required to transfer that individual's digital personal information to another organization in a structured, commonly used, and machine-readable format when it is technically feasible (data portability)? **This is a few of what ifs, an individual hopefully is capable of submitting the data themselves. Request a copy or scan then the person/individual submits it themselves to the other party.**

3. Should organizations be required to provide individuals with the logic involved in automated decision making about that individual (algorithmic transparency)? **Yes, I would prefer this for myself**

Page 21 Questions: 1. Should PIPA regulate the de-identification and/or anonymization of personal information within the control of an organization and the subsequent use or disclosure of the de-identified or anonymized information? If so, how? **Do what you do for minors,**

2. Should organizations be required to have a privacy management program and provide written information about the program to individuals and the Commissioner? **Yes and hopefully this sets Person's mind at ease that in no way are the organizations able to sell the person's information to anyone and/or business even if online such as follows: e-business.**

3. Should organizations be required to complete and submit a privacy impact assessment to the Commissioner for specific initiatives involving personal information? **The more information the better, since some businesses are not very open at how they conduct business, person's private information might be sold to a third party for money to that company/business.**
Page 22 Question: Are the provisions for notification of breaches to the Commissioner and individuals under PIPA appropriate? **No for the cooperation is suppose to notify you however they could be the ones doing the breaching, identity theft. Then what?**
Page 23 Question: Should PIPA include the ability of the Commissioner to levy administrative monetary penalties against an organization for certain contraventions of the Act? **Yes**
Thank you
Love from Judith Knight John Oliver Cromwell representative plus inheritor and a whole lot more
Appendix A – Jurisdictional Summary Tables of Emerging Issues Table 1 Application of Selected Privacy Legislation GDPR CPPA QPSA AB PIPA Whenever personal data of individuals located in the EU is processed To federal works, undertakings, and businesses that are within the jurisdiction of parliament; and to organizations, including an association, a partnership, a person or a trade union, in respect of personal information that the organization collects, uses or discloses in the course of commercial activities. To organizations based and operating in Quebec. The Act also applies to personal information held by a political party, an independent Member or an independent candidate to the extent provided for by the Election Act. To organizations that collect, use, or disclose personal information in Alberta, meaning: • a corporation, • an unincorporated association, • a trade union • a partnership • an individual acting in a commercial capacity, • and certain non-profit organizations when acting in a commercial capacity
Table 2 Scope of Selected Privacy Legislation GDPR CPPA QPSA AB PIPA Whenever personal data is processed. "Processing" is a broad term that covers almost anything that can be done with data, whether or not by automated means, including collection, storage, transmission, and analysis, etc. Whenever personal data is collected, used, or disclosed Whenever personal information is collected, held, used or communicated to third persons in the course of carrying on an enterprise.* Whenever personal information is collected, used, or disclosed * The definition of "enterprise" is set out in s. 1525 of the Civil Code of Québec, CQLR c. CCQ 1991 as "[t]he carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service." 25 Table 3 Definition of Personal Information in Selected Privacy Legislation GDPR CPPA QPSA AB PIPA Information relating to identified or identifiable person Information about an identifiable individual Includes provisions with respect to personal employee information of any federal works, undertakings, and businesses that are within the jurisdiction of the Parliament of Canada. Personal information "is any information which relates to a natural person and directly or indirectly allows that person to be identified." Information about an identifiable individual Includes provisions with respect to personal employee information in Alberta organizations. Table 4 Provisions for Sensitive Personal Information in Selected Privacy Legislation GDPR CPPA QPSA AB PIPA The GDPR sets

out additional protections for “special personal data” relating to sensitive personal information: data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; and data concerning health or sex life and sexual orientation; genetic data or biometric data. Children have specific protections for their personal data. Personal information of minors is considered “sensitive information” and children have specific protections for their personal data. Sets out additional protections for “sensitive personal information” defined as information that “due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or communication, entails a high level of reasonable expectation of privacy.” Includes protections for personal information collected using technology that allows the person concerned to be “identified, located, or profiled.” Minors under 14 years of age have specific protections for their personal information. None. 26 Table 5 Forms of Consent Provided for in Selected Legislation GDPR CPPA QPSA AB PIPA Consent means any “freely given, specific, informed, and unambiguous indication of the data subject’s wishes by a statement or clear affirmative action” agreeing to the processing of their personal data. Explicit consent is required for processing special categories of data; for automated individual decision making, including profiling; and for international data transfers. Permits: • express consent and • implied consent. This is measured on a level of reasonableness and considers the sensitivity of the information. Consent must be obtained in plain language. Permits: • Express consent that “must be clear, free and informed and be given for specific purposes.” Express consent is required for “sensitive personal information.” Consent must be obtained in “clear and simple language.” Permits: • express consent, • deemed consent, and • opt-out consent (when consent is presumed, but an individual can decline). Consent is measured on a level of reasonableness. Table 6 Rights Defined in Selected Privacy Legislation GDPR CPPA QPSA AB PIPA The GDPR is rights-based legislation and directly prescribes the following: • Right to be informed • Right to access • Right to correction of personal information • Right to erasure • Right to restriction of processing • Right to data portability • Right to object to data processing activities Right to logic behind automated decision systems The preamble to Bill C-27 refers to rights. In addition, the provisions of the CPPA appear to provide for an individual’s: • Right to be informed • Right to access • Right to request correction of personal information • Right to disposal of personal information • Right to data portability if a data mobility framework is in place between organizations • Right to logic behind automated decision making Individuals have the right to withdraw or change consent. • Right to be informed • Right to access • Right to request correction of personal information • Right to erasure • Right to logic behind automated decision systems Individuals have the right to withdraw consent. Alberta’s PIPA establishes consent as the primary mechanism by which individuals may use to control the collection, use and disclosure of their personal information by organizations. The provisions of PIPA do not refer to rights. Nevertheless, PIPA provides an individual’s: • Right to be informed • Right to access personal information • Right to request correction of personal information • Right to request information about the use and disclosure of personal information Individuals have the right to withdraw or change consent. 27 Table 7 Anonymization and De-identification of Personal information in

Selected Privacy Legislation GDPR CPPA QPSA AB PIPA Provides rules for the use of "pseudonymized data" – that is personal information processed in such a manner that the personal data can no longer be used to identify an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that identification is impossible. Personal information may be used without consent if the information is de-identified for internal research, analysis, and development. Personal information may be used without the consent of the person concerned for the specific purposes of research or for the production of statistics and if the information is de-identified. No provision. Table 8 Provisions for Privacy Management Programs in Selected Legislation GDPR CPPA QPSA AB PIPA The GDPR provides for privacy by design and by default. Organizations must "implement appropriate technical and organisational measures" to protect personal information that take into account "cost of implementation and the nature, scope, context and purposes of processing as well as the risks" to the individual involved. Every organization must implement and maintain a privacy management program that includes the policies, practices, and procedures the organization has in place to fulfill its obligations under the Act. On the request of the Commissioner, the organization must provide the Commissioner with access to the policies, practices and procedures that are included in its privacy management program and provide guidance on or recommend that corrective measures to its privacy management program. Any person carrying on an enterprise must establish and implement governance policies and practices regarding personal information that ensure the protection of such information. Such policies and practices must provide a framework for the keeping and destruction of the information, define the roles and responsibilities of the members of its personnel throughout the life cycle of the information and provide a process for dealing with complaints regarding the protection of the information. • The policies and practices must be published in clear language on the organization's website. An organization must designate individual(s) to provide oversight for PIPA compliance and develop and follow policies and practices that are compliant. The organization must provide written information about those policies and practices upon request. Policies and practices must include information on collection, use and disclosure and the purposes for which a service outside of Canada is used, if relevant. 28 Table 9 Provisions for Privacy Impact Assessments in Selected Legislation GDPR CPPA QPSA AB PIPA Mandatory before initiating any processing that may have a high risk of infringing on individual rights Organizations relying on the legitimate interest exception will be required to complete a privacy impact assessment and to provide copies of the assessment to the Commissioner on request. Mandatory "for any project to acquire, develop or overhaul an information system or electronic service delivery system" involving personal information." Table 10 Provisions for Breach Notifications in Selected Legislation GDPR CPPA QPSA AB PIPA Notification required within 72 hours to the Commissioner in each country (called the "supervisory authority"), and to individuals "without undue delay" when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. Notification required as soon as it is feasible to the Commissioner and to the individual if it is reasonable to believe that the breach creates a real risk of

significant harm to the individual. The Commission d’accès à l’information and the affected individual must be notified promptly if the incident presents a risk of serious injury. Notification is required to the Commissioner without unreasonable delay if the breach poses a real risk of significant harm to the individual. The Commissioner may then require the organization to notify individuals affected by the breach and to do so within a specified period of time. Table 11 Provisions for Administrative Monetary Penalties in Selected Legislation GDPR CPPA QPSA AB PIPA Serious infringement: up to 20 million Euros or four per cent of annual worldwide turnover. Lesser infringement: up to 10 million Euros or two per cent of annual worldwide turnover. Maximum penalty of the higher of $10 million or three per cent of the organization’s annual gross global revenue. Maximum penalty of $50,000 in the case of a natural person and, in all other cases $10 million or, if greater, the amount corresponding to two per cent of worldwide turnover for the preceding fiscal year. None. Sources: Office of the Information and Privacy Commissioner for British Columbia, Guidance Document: Competitive Advantage Compliance with PIPA and the GDPR, March 2018, p. 2, available at \\zeus.lao.local\shared$\COMMON\LIBRARYHS\Research\Committees\LPCs\AB's Economic Future\PIPA\PIPA 2022\Reviews and Reports\BC_PIPAReview_2020- 21\GD GDPR vs PIPA March 2018.pdf (accessed August 25, 2022); House of Commons of Canada, Bill C-27, available at https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/firstreading (accessed September 15, 2022); Alberta, Personal Information Protection Act, S.A. 2003, c. P-6.5; Quebec, Loi sur la protection des renseignements personnels dans le secteur privé/Act respecting the protection of personal information in the private sector, CQLR c. P.39-1.