IIACACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

701 WEST GEORGIA STREET | SUITE 1500
VANCOUVER, BC | V7Y 1C6

604.637.1676 | www.iiac.ca

Susan Copland, LLB, BComm
Managing Director
scopland@iiac.ca

August 10, 2021

Manager of Access and Privacy Strategy and Policy Unit
Ministry of Government and Consumer Services
Enterprise Recordkeeping, Access and Privacy Branch

Email: access.privacy@ontario.ca

Dear Sir/Madam:

Re: Public Consultation – Modernizing Privacy in Ontario (the "Consultation")

The Investment Industry Association of Canada (the "IIAC") appreciates the opportunity to participate in the Consultation. The IIAC is the national association representing 116 investment dealer firms, on securities regulation and public policy. Our members are the key intermediaries in Canadian capital markets, accounting for the vast majority of financial advisory services for individual investors, and securities trading and underwriting in public and private markets for governments and corporations.

IIAC members provide financial advisory services to millions of Canadians, collectively holding 6,615,000 full-service brokerage accounts, as well as many other self-directed, digital, and hybrid accounts. In servicing these accounts, our industry is responsible for safeguarding some of our clients' most sensitive personal information, including the details of, and access to their accounts and financial data.

As stated in our submission dated October 1, 2020, responding to Ontario's Consultation on Strengthening Privacy Protections in Ontario, IIAC recognizes the importance of having a robust and comprehensive regulatory regime to ensure the privacy of individuals is protected. In order to protect this critical data, investment dealers have developed robust data protection processes and safeguards within their firms, and in their interaction with third party processors. The industry has also worked closely with its regulator, the Investment Industry Regulatory Organization of Canada ("IIROC") to ensure clients benefit from appropriate protection of their data.

We believe that the best way of protecting personal information is for Canadian jurisdictions to adhere to the existing federal legislation, as is currently the case for Ontario businesses that are subject to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). PIPEDA has proven to be a practical, established, and well-understood framework for companies and individuals whose information is protected.

We are concerned that the further expansion of the provincial patchwork of privacy rules will introduce additional regulatory inconsistencies which will in turn increase uncertainty, create inefficiencies, and increase the cost of compliance for Canadian entities operating within and outside of Canada, and foreign entities seeking to do business in Canada.

Aside from complicating and increasing the cost of trade within Canada, having different privacy regulations within Canada may negatively affect our collective ability to obtain the necessary "adequacy recognition" under the European *General Data Protection Regulation* ("GDPR") and other international regulations, in a timely manner. This would affect businesses' ability to efficiently conduct business with Europe and other international jurisdictions. The need to obtain an adequacy ruling from the EU for the regulatory regime in each province, in addition to the federal government, increases the complexity and uncertainty that Canada as a whole will be deemed to have equivalent regulatory protections.

Rather than creating a new legislative framework and the bureaucratic infrastructure to support new Ontario regulation, we strongly recommend that where there are perceived gaps relating to certain provincial entities, they be dealt with on a targeted basis, using the provisions in PIPEDA, or Bill C-11, if enacted, as a template for the way in which these situations are handled.

Should a separate Ontario regulation be enacted, the result would be that Canada would have 5 different private sector privacy laws, in addition to the 30 other privacy related regulations dealing with specific concerns and sectoral areas of privacy. This proliferation of regulation imposes an immense regulatory burden on companies that must ensure they understand each specific regulation, where they intersect and are overridden by each other, and then build systems to ensure they comply with all laws in each situation where Personal Information is involved.

We note that the Consultation does not speak to the need for harmonization among provinces and the federal legislation, or a domestic recognition framework that would simplify the regulatory complexity of dealing with several regulators for the same issues, particularly if there is a security incident.

Ultimately, this would lead to an untenable situation, and is particularly out of scale for a country the size of Canada.

If Ontario elects to create its own separate privacy regime, we urge the Ontario Government to work with the Department of Innovation, Science and Economic Development Canada ("ISED") and the relevant provincial regulators in British Columbia, Alberta, and Quebec to develop a harmonized privacy regulatory framework uniformly applicable across Canada. Currently, the provincial and federal privacy laws are relatively consistent in terms of content and outcomes. A harmonized approach would also facilitate a simplified interface with the GDPR and other international regulatory regimes that recognize regimes with similar protections.

Our comments on the specific provisions of the proposed regime are as follows:

Rights Based Approach

Although we acknowledge that the GDPR takes a rights-based approach to privacy, it is not clear that such a framework will result in a higher level of privacy protection for individuals. The Consultation does not articulate specifically why a rights-based framework is needed, and how the absence of this approach in existing regulation has impaired individuals' privacy rights.

We are concerned that framing the legislation within a rights-based framework will override the existing and necessary regulatory approach in PIPEDA and provincial privacy regulation, that counterbalances privacy protections with commercial interests that include fostering innovation, maintaining competitiveness and facilitation of efficient business. It should be noted that Canadian courts currently apply a legal test which balances the interests of consumers with the legitimate business needs of an organization. As such, framing privacy as a human right would not add material protections.

Rather than re-framing the regulation without consideration of the effects on the economic impact, we recommend that an analysis be undertaken examining where shortcomings in privacy protection exist without the rights framework. If gaps exist, we recommend that they be rectified within the current regulatory framework. This would preserve the critical balance that recognizes the commercial and competitive context in which the digital ecosystem operates.

Fair and Appropriate Purposes

Existing Canadian privacy regulation contains provisions that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. We are concerned that the addition of the word "fair" introduces uncertainty without a clear regulatory benefit. Whereas there is existing guidance and decisions interpreting what reasonable and appropriate comprises, introducing the new element of "fair" is certain to result in confusion, uncertainty and greater disharmony across Canadian privacy regimes. The "factors to consider" articulated in subsection (2) are sufficient to clarify what are "appropriate circumstances", without the addition of the additional and uncertain qualifier of "fair". "In subsection (3), it would be helpful to qualify the definition of "purpose" as something that is not materially different or inconsistent with the current use of the data. The use of technology can often result in new revelations and insights which may be used to enhance the service offering to the individual. Requiring an organization to determine at or before the time of the collection of any personal information, each of the purposes for which the information is to be collected, used, or disclosed and record those purposes, may not (always) be practical and possible to operationalize.

The addition of subsection (4), which specifically excludes certain activities from "legitimate needs" introduces prescriptive and problematic limitations on current and future uses of data. The strength and long-term relevance of PIPEDA is in large part due to its principles-based drafting, and avoidance of regulation of specific uses of data. The activities articulated in subsection (4) would capture activities that are outside the areas of concern and would likely include socially beneficial activities. By restricting monitoring and profiling, the regulation would disallow evaluation, analysis, and prediction of activities for individuals under 16 years old. This evaluation, analysis and prediction is in itself not an issue; it is the actions taken using such data. Restricting the collection and analysis would have counterproductive effects when such analysis is undertaken for socially responsible objectives, including medical advancements and diversity and equality initiatives. It is critical that the legislation focus on the outcomes it seeks to achieve, not the potential means of achieving them, which is certain to preclude activities that lead to beneficial outcomes. In this case, the "reasonable and appropriate" standard is sufficient to preclude the negative outcomes anticipated by the proposed legislation.

Limiting collection, use and disclosure

We are concerned that the requirement that the data collected must be "necessary" for purposes determined may unduly qualify the Appropriate Purposes standard. We note that this is also a higher

standard than the PIPEDA "reasonableness" standard. It is unclear how "reasonable" will be differentiated from "necessary", and who will make those distinctions.

Disposal at individual's request

The Consultation poses the question about whether the right of erasure should include all information that an organization holds about an individual, including from third parties such as data brokers, rather than information that was collected from them directly. We are concerned that such a broad erasure requirement could be problematic, particularly in an organization with many divisions and where information is used for different purposes. Deleting information for one purpose might affect its necessity in another area for which the client is unaware. In addition, where divisions of firms may be segregated, personal information about a client in one division may not be knowable or accessible by another divisions. In respect of data not provided by the client, we are concerned that there is a potential for this to include derived data or data produced by the use of analytics. Where such data is used to develop modeling or other analytics, it may not be possible to separate that data from the aggregate that is used to undertake the analytics or develop the model.

In drafting the provisions related to disposal, regulators should also consider the possibility that unscrupulous individuals may request disposal to avoid fraud detection or anticipated litigation.

We believe the strong accountability obligations contained in Canadian legislation, in addition to the provisions requiring retention only as long as necessary to fulfill the intended purposes, along with the complaint mechanisms contained in the legislation mitigate the need for such a broad-based disposal right.

Disposal by service provider

We agree that individuals should be able to require that their data is disposed not only from the primary organization but also their service providers. However, the requirement that the organization must *ensure* that the service provider disposes of the information should be replaced with a provision that requires that they take reasonable steps to ensure the service provider dispose of the information. Given that the organization does not have direct access to the systems of the service provider, they cannot fully ensure that data has been disposed of.

Data Mobility

We support the proposal that a data mobility framework be imposed on an industry-by-industry basis, to allow for the unique manner in which each industry uses data, and the different technology systems and protocols that are common within each industry. It is critical that the data to be subject to the mobility framework should be restricted to the personal information relating to the individual, which was provided by the individual to the organization, and not include any derived data or inferred information. Including such information would be practically unworkable, as given the variable nature of such information, there would be a lack of uniformity within and between organizations. The unique nature of the information would preclude such information from being built into a uniform framework. In addition, including such data may reveal competitive information about products and services that are developed using client data. It would also include analysis required for the purposes of conducting due diligence (e.g. Know Your Client, client authentication, etc.), which would be of little value as it is incumbent on each organization to conduct this independently.

Automated decision systems

We note that the broad definition of automated decision systems captures virtually all systems and decisions where data is used, including for purely administrative functions. This would result in voluminous disclosure, rendering the requirement meaningless. Such a requirement represents a departure from the GDPR, which allows decisions that are *solely* automated to be questioned.

The proposed wording prohibiting the use of automated decision making is very problematic, in that it includes profiling, which involves data analysis, but does not involve a decision or action that may affect the individual. As well, broadening the definition to include any automated decisioning that assists humans can result in significant operational burden if there are not appropriate materiality limits in place.

The proposal contains a requirement that that automated decision systems not be used if the decision would "significantly affect" the individual unless the decision is necessary to fulfill the contract, authorized by law or the organization obtains express consent. It is critical therefore to define "significantly affect", with the inclusion of examples.

The requirement that the organization provide individuals, on request, an explanation of the prediction recommendation or decision, and how personal information was used to make it is also impractical, as the broad definition of automated decision system does not limit this requirement to material decisions. This could lead to nuisance requests about how non-material information is processed and decisions are made and would require firms to use time and resources to set up a system to manage such requests. We recommend a materiality standard be applied so that only decisions that have a significant impact on individuals could be subject to this provision.

The requirement to provide an explanation of how the system uses the information to make predictions may be difficult or impossible to implement, in respect of the use of artificial intelligence. The nature of artificial intelligence is that it uses vast amounts of data to make connections that are not necessarily predictable. Artificial intelligence systems utilize information from varied sources, some of which may not seem relevant, to make connections and render decisions. The value of artificial intelligence is its ability to make such connections that humans are incapable of making, so that it may not be clear what information is being used. As such, only a broad statement and prediction as to how an organization expects that the data will be used may be possible.

We are concerned that the proposed transparency provisions for this right are quite unique relative to other jurisdictions. As a result, organizations may choose not to invest anew in such processes or technology if the compliance burden is believed to be too high. This would be contrary to the whitepaper's introductory statement of "...make Ontario the world's most advanced digital jurisdiction."

Consent

We agree with the position in the Consultation that the modern data landscape is too complex to rely upon consent as the authority for data collection and use. The problems of consent fatigue and the issues with long, legalistic privacy notices are well articulated.

We support allowing organizations to rely on implied consent in some circumstances, taking into account the sensitivity of the information and the reasonable expectations of the individual. We are, however, concerned with the wording that says the personal information should not be collected for the purposes

of influencing the individuals' behavior or decisions. It is not clear if that applies to the recommendation of products and services within the ambit of the services for which the individual contracted, such as investment services. In addition, in the financial industry for instance, there are many valid use cases for personal information, (e.g. beneficiary information, e-transfer/wire payment recipients, emergency contact information, information on spouses, dependents, for purposes of financial planning, etc.). Collecting personal information assists advisors in carrying out the expected services, and identifying the most appropriate products and services for their clients, and this use would be reasonably expected by clients.

Privacy by Design

We are supportive of a requirement for that companies should undertake Privacy Impact Analyses, and in certain circumstances, implement Privacy by Design. These requirements should be subject to a materiality threshold, so that they would only be required where the volume, sensitivity and nature of the data would justify the implementation of such safeguards.

Oversight Body

It is appropriate that the Commission be empowered to oversee the regulations, and issue orders, similar to framework that exists in British Columbia and Alberta. We do, however, favour the approach proposed in Bill C-11, which would create a tribunal structure to review and enforce the recommended penalties. This separation of powers is an appropriate structure to help ensure due process, in that it removes the conflict of interest in having the same body investigate, recommend, and impose penalties. The Tribunal, which would include subject matter experts on the panel, introduces an objective review, and would result in more confidence in the ultimate decisions. This is particularly important given the significant fines that could be issued in the event of a breach of the regulation. The quantum of such fines could quite possibly shut down a business or an industry. It is appropriate that the Commission consider the various factors articulated in subsection (3) in making a determination of the amount of the administrative penalty, however the wording should mandate the consideration of these factors.

Specifically articulating such considerations will promote confidence, if the decisions clearly state how these factors apply to their decisions. Where there is transparency about how these factors impact decisions, organizations can also make better decisions about their activities.

We are concerned that the Consultation suggests that there is only a right of appeal where it pertains to questions of law and does not allow for appeal of the quantum of a fine. Given the potential quantum of the fine, as well as the possibility that it could be multiplied by the other provincial and federal regulators, it is appropriate that appeals should be allowed to be based on questions of fact, as well as fairness of the recommended penalty.

We are concerned with the quantum of the maximum administrative penalty. Although the Proposal indicates that this penalty is to encourage compliance and not to punish, the potential for a fine that is the higher of $10,000,000 or 3% worldwide revenue could very well be considered punitive. Given that the Commission is not bound by the rules of evidence, the potential for such fines seems to violate the principle of due process.

We are also concerned about the significant potential penalties for offences under the Proposal.

We note that an offence is punishable by fines of up to $25 million / 5% revenue or $20 million. These fines are significant, particularly in light of the lack of strong due process controls. It is also not clear if the mitigating factors and appeal mechanisms apply to the statutory offence penalties. Such due process provisions are critical given the potential quantum of such penalties, including the proposal to order that individuals be compensated by the organization.

Codes of Practice/Certifications

We are strongly supportive of the provisions in the Proposed Act that allow for the creation of codes of practice and certifications. The manner in which different industries manage personal information can be very different, yet still comply with the spirit and letter of the legislation. The structure of the regulation as principles-based makes it conducive to the use of codes and certifications. It also may alleviate the administrative burden of the Commission in overseeing the regulation, as governing bodies with expertise in the particular industry, and the way in which personal information is, and should be used, can make appropriate decisions and observations about the manner in which entities in that industry are, or are not, complying with the law. Certification and industry codes will assist establishing and governing data mobility frameworks, use of algorithms, the use of artificial intelligence, cybersecurity standards and de-identifying processes. This will limit liability and promote consistency where firms are following codes and certifications.

We also support the enforcement implications, where organizations complying with industry codes would not be subject to the administrative penalties. This is fair and appropriate, recognizing that the codes, as approved by the Commission, form the regulatory framework under which the participating organizations operate, and firms should not be penalized if they are in compliance with those codes.

It is critical that there be multi-jurisdictional coordination not only in the application of the explicit provisions in the legislation, but also in respect of the use of industry codes. There must be some form of a coordination of orders and penalties in the case of an organization using such codes and operating in multiple provinces. Without, there is a risk of cumulative penalties that collectively may be unreasonable for an individual incident, or to a series of disparate or contradicting orders that are challenging to implement/operationalize.

De-identified Information

It is critical to build in provisions that balance need for personal information to support technology while protecting personal information. We appreciate that the proposed definition of de-identified information supports pseudonymization and anonymization and recognizes that the information can be re-identified with the use of other information, which allows for the spectrum of identifiability. It is important that the legislation permit organizations to use de-identification and subsequent re-identification as a means for safeguarding personal information at rest or in transition, without requiring consent. This should also include an exemption to use de-identified information for internal analytics (e.g. analytics required to support operations such as fraud models, pricing models and risk models), without requiring consent.

In order to provide clarity, de-identified information should not be in scope of the definition of personal information and therefore be exempt from disposal and access requests.

Conclusion

The appropriate protection of personal data is of utmost importance to the investment industry. Investment firms fully recognize the value and sensitivity of the data entrusted to them, and the industry has implemented significant and robust data protection processes. In order to best protect clients' data, it is critical that the regulatory measures are structured to facilitate efficient compliance. Implementation of a patchwork of different provincial regulations with varying standards is a barrier to efficient and effective compliance. We believe that a singular Canadian approach to privacy regulation, either through an overarching regulatory structure, or at a minimum, through harmonized regulation best serves this objective.

Thank you for considering our comments. If you have any questions, please don't hesitate to contact me.

Yours sincerely,

Susan Copland