VIA INTERNET PORTAL

July 29, 2021

Special Committee to Review the *Personal Information Protection Act*

Dear Special Committee members,

Re: Modernizing the *Personal Information Protection Act*

The Portfolio Management Association of Canada (**PMAC**) is pleased to have the opportunity to respond to British Columbia's (**BC**) request for comments on modernizing the *Personal Information Protect Act* (**Consultation**). PMAC is supportive of BC's efforts to enhance British Columbians' individual privacy rights, while providing the appropriate flexibility within a harmonized national privacy framework to allow our member firms to serve investors in Canada and across the globe.

PMAC represents over 300 investment management firms – both Canadian and foreign - registered to do business in Canada as portfolio managers (**PMs**) with the members of the Canadian Securities Administrators (**CSA**) from coast-to-coast. In addition to this primary registration, most of our members are also registered as investment fund managers and/or exempt market dealers (we refer to these entities collectively herein as **asset managers**). PMAC's members include large and small firms, managing total assets in excess of $2.9 trillion for a variety of Canadian investors, ranging from pension plans and sophisticated institutions to individual Canadians. PMAC's members include fully on-line asset manager models to hybrids and more traditional firms.

OVERVIEW

PMAC's mission statement is "advancing standards"; we are consistently supportive of measures that improve standards for the benefit of investors (the clients of asset managers). Clients choose to invest their assets with portfolio managers for a number of reasons, including the fact that clients delegate the responsibility for asset management to PMs on a discretionary basis. This means that PMs do not check in with their investors for every transaction they make in a client's account. Rather, PMs have the authority to act on the client's behalf – and in their best interest. Ensuring broad access to discretionary investment management through a wide variety of

portfolio manager business models – including on-line and traditional – is beneficial to Canadians and to the Canadian economy. As is further discussed below, privacy laws must be sufficiently flexible to ensure that PMs are able to carry out their responsibilities to clients without undue restrictions, such as the need to frequently obtain client consent.

PMAC has been supportive of proposals that provide assurances to individuals that their privacy is protected, that their data will not be misused, and that companies communicate privacy matters in a simple and straightforward manner. We agree that BC's privacy regime should be modernized and streamlined in a way that simultaneously supports innovation and protects the privacy expectations of British Columbians.

KEY RECOMMENDATIONS

PMAC's key recommendations are as follows:

- **Await the enactment of the Federal *Digital Privacy Implementation Act* (Bill C-11)** and focus efforts on advocacy at the Federal level to ensure that any gaps identified in Bill C-11 are dealt with at a national level. British Columbia should align its privacy legislation as much as possible with the Federal legislation.

- **Harmonize legislation between provinces and federally** to allow firms that operate in multiple jurisdictions to operate seamlessly across Canada. This will reduce costs and improve efficiency for businesses, and lead to improved compliance and enhanced consumer protection. The legislation should also be aligned with other jurisdictions, particularly Canada's major trading partners, such as the European Union, the United Kingdom, and the United States.

- **Adopt a principles-based approach**. Privacy laws should be robust, transparent and clear. BC's privacy law should foster innovation, competition, and equivalency with other jurisdictions, while also providing improved privacy protection and clarity about compliance.

- **Provide for a staged implementation** if BC decides to update its privacy legislation, substantial changes may be needed for businesses to enhance and improve their privacy programs. This will require significant time, resources, and capital. We therefore ask that a staged implementation period of at least 2 years be considered to allow firms, and smaller businesses in particular, to adapt to these new regulatory requirements.

Harmonization

We wish to emphasize the critical importance of harmonizing privacy legislation across Canada. As noted by the Office of the Information & Privacy Commissioner for British Columbia, "…harmonization among federal and provincial laws benefits both businesses and individuals."[1] A lack of harmonization creates consumer confusion, presents a significant hardship to PMAC members that operate nationally and internationally, threatens innovation and competition, and ultimately has a negative impact on the British Columbian and Canadian economies. We believe that individuals should be entitled to similar privacy protections regardless of their jurisdiction of residence.

It is not desirable to have a patchwork of compliance requirements in various Canadian provinces. This makes compliance difficult, adding costs and regulatory burden that are disproportionate to the privacy protection gaps identified. The risk of inadvertent non-compliance increases, which can result in regulatory enforcement, penalties, and litigation. Ultimately this does not best achieve the consumer protection goals of privacy legislation.

It would be advisable for BC to await the enactment of the new Federal privacy legislation before proceeding with provincial legislation. Even provincial legislation that is aligned with the Federal legislation subjects organizations to an additional compliance regime in the province. This represents additional cost and regulatory burden to firms, without substantial added consumer protection. We therefore encourage BC to work with the Federal government to eliminate any identified gaps in Bill C-11. We urge BC to align its proposals to the Federal legislation to better harmonize requirements across Canada. We encouraged Quebec to do the same in our comments to the Quebec government on Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, and will take the same position in our response to the current Ontario privacy law consultation.

Bill C-11

The Consultation asks that comments focus on the provisions in Bill C-11 and the General Data Protection Regulation (EU) (**GDPR**), as well as on the Office of the Information and Privacy Commissioner for British Columbia's recommendations to the Committee. We noted in our comments on Bill C-11 that we were pleased to see that the proposed consent and transparency provisions reflect much the same approach as those adopted under the GDPR, as well as some privacy law in the United States. This harmonization is essential to maintaining Canada's equivalency standard in other jurisdictions and ensuring our international competitiveness.

[1] Office of the Information & Privacy Commissioner for British Columbia, Supplemental submission to the Special Committee to Review the Personal Information Protection Act, February 23, 2021 at page 2

Rather than repeat them here, we have attached a copy of our comments on Bill C-11 for your review. We ask that you consider these comments in deciding how best to modernize BC's legislation.

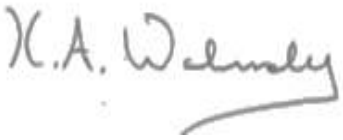
CONCLUSION

We are supportive of updating privacy legislation to improve clarity and consistency and advance privacy protection standards for Canadians, including British Columbians. Privacy legislation should be robust, transparent, and must be aligned from coast-to-coast to protect individuals, support businesses, and ensure our competitiveness and attractiveness with trading partners. For asset managers, we believe that a reasonableness standard, exemptions to the consent requirements, and a principles-based framework are required to allow firms to tailor their policies and procedures to the type and quantity of information they collect, and to facilitate the use of personal information for the benefit of investors. We urge BC to await the outcome of Bill C-11 before deciding whether to update its provincial privacy legislation and what to include in any such amendment.

Thank you for the opportunity to respond to the Consultation. If you have any questions regarding the comments set out above, please do not hesitate to contact Katie Walmsley at (416) 504-7018 or Victoria Paris at (416) 504-1118.

Yours truly,

PORTFOLIO MANAGEMENT ASSOCIATION OF CANADA



Katie Walmsley
President

Margaret Gunawan
Director
Chair of Industry, Regulation & Tax Committee,

Managing Director – Head of Canada Legal & Compliance
BlackRock Asset Management Canada Limited

Encl.

VIA EMAIL: ISI.minister-ministre.ISI@canada.ca

March 12, 2021

Minister of Innovation, Science and Industry
The Honourable François-Philippe Champagne
C.D. Howe Building
235 Queen Street
Ottawa, Ontario K1A 0H5

Dear Minister Champagne,

Re: *Digital Charter Implementation Act, 2020* (Bill C-11)

The Portfolio Management Association of Canada (**PMAC**) is pleased to have the opportunity to submit the following comments regarding the *Digital Charter Implementation Act, 2020* (**Bill C-11**). PMAC is supportive of the enactment of the *Consumer Privacy Protection Act* (**CPPA**) and the *Personal Information and Data Protection Tribunal Act* (**Tribunal Act**). We believe these initiatives strike the correct balance between the protection of individual privacy while providing the appropriate flexibility for our member firms to serve investors in Canada and across the globe.

PMAC represents over 285 investment management firms – both Canadian and foreign - registered to do business in Canada as portfolio managers with the members of the Canadian Securities Administrators (**CSA**). In addition to this primary registration, most of our members are also registered as investment fund managers and/or exempt market dealers (we refer to these entities collectively herein as **asset managers**). PMAC's members include large and small firms, and "traditional" as well as on-line firms, managing total assets in excess of $2.7 trillion for a variety of Canadian investors, ranging from pension plans and sophisticated institutions to individual Canadians.

OVERVIEW

PMAC's mission statement is "advancing standards"; we are consistently supportive of measures that improve standards for the benefit of investors (the clients of asset managers). Portfolio managers have a fiduciary duty to act with care, honestly and in good faith, always in the best interest of their clients, and securities regulation requires that portfolio managers have the highest levels of education and experience

in the investment industry. Portfolio managers provide ongoing management of clients' investments, on a discretionary basis, based on objectives and risk tolerance outlined in the client's Investment Policy Statement (**IPS**). Ensuring broad access to discretionary investment management through a wide variety of portfolio manager business models – including on-line and traditional – is beneficial to Canadians and to the Canadian economy. As is further discussed below, privacy laws must be sufficiently flexible to ensure that PMs are able to carry out their responsibilities to clients without undue restrictions, such as the need to frequently obtain client consent.

As set out in our September 2019 comment letter on the discussion paper *Strengthening Privacy for the Digital Age* (the **2019 Consultation**), we applaud the Federal government's aim of ensuring that Canadians can trust that their privacy is protected, that their data will not be misused, and that companies communicate privacy matters in a simple and straightforward manner. We agree that Canada's privacy regime should be modernized and streamlined in a way that simultaneously supports innovation and protects the privacy expectations of Canadians.

KEY RECOMMENDATIONS

PMAC's key recommendations are as follows:

- **PMAC agrees with the reasonableness standard and principles-based approach** taken to privacy in the CPPA. PMAC believes that Canada's privacy legislation must be robust, transparent, and aligned with other jurisdictions, particularly our major trading partners, such as the European Union, the United Kingdom, and the United States. In our view, the CPPA provides a balanced approach to updating Canada's privacy laws in a way that fosters innovation, competition, and equivalency with other jurisdictions, while also implementing needed enhancements to privacy protection and clarity about compliance.

- **PMAC supports the proposed exemptions to the consent requirement** to facilitate the use of personal information by firms under certain circumstances, including for standard business practices. We agree that knowledge and consent should not be required when transferring information to a service provider. We believe these exemptions to be beneficial for asset managers, as well as for investors. We further believe this will be advantageous to Canadian businesses from an international competitiveness and comparability perspective. It will also assist individual consumers whose consent is sought for the collection, use and disclosure of their personal information to be able to focus on what is truly important, without the distractions that lead to "consent fatigue".

- **PMAC agrees that codifying existing guidance and interpretation will provide certainty, improve compliance, and advance standards** with respect to information management and privacy protection. However, the substantial changes that may be needed for businesses to enhance and improve their privacy programs will require significant time, resources, and capital. We therefore ask that a staged implementation period of at least 2 years be considered to allow firms, and smaller businesses in particular, to adapt to these best practices.

SPECIFIC COMMENTS RELATING TO THE CPPA AND THE TRIBUNAL ACT

We have the following comments on certain aspects of the CPPA and the Tribunal Act.

Concept of "control"

We agree in principle with the notion that an organization should be accountable for information that is under its control. However, our members question the drafting of s. 7(2) of the CPPA because an organization may not "decide" to collect certain information and may not be in a position to "determine the purposes of its collection, use or disclosure" – for example, the organization be required to collect, use or disclose information by statute or otherwise. We therefore suggest that the section be re-drafted to remove the subjective component, and/or provide additional clarity that the organization is accountable for information that is under its control, regardless of who "decides" to collect it.

In the context of asset managers, the CSA require portfolio managers to collect prescribed information about each client for the purposes of "knowing the client" and to assess the suitability of the investment decisions made by the firm on behalf of its clients. The information required to be collected and documented is extensive and includes details about clients' personal financial circumstances and risk profile (a combination of risk tolerance and risk appetite). Additionally, under anti-money laundering and anti-terrorist financing laws (collectively, **AML**), firms have an obligation to collect and, in some instances, to report, information about clients' identities, the source of their funds and whether a client is a "Politically Exposed Person" (**PEP**). This information can be very sensitive, but is information that is required by law to be collected, as opposed to information that the firm "decides" to collect.

We agree that "control" should remain with the organization where information is transferred to a service provider, and we agree that client knowledge and consent should not be required when transferring information to a service provider, with applicable limits, as further discussed below.

Consent and transparency

PMAC supports the exception from express consent for a collection or use of personal information for legitimate business activity. We agree that consent requirements should be focused on areas where the impact is greatest, that consent should be meaningful, and that it is important to be wary of "consent fatigue". This is particularly relevant in the investment industry, where investors are already provided with extensive disclosure about investment products, risks, relationships, and conflicts of interest.

The ability to transfer information to a third-party service provider for processing without the individual's knowledge or consent will allow firms to select and change service providers in a timely fashion to address technology, security, cost, innovation – or other concerns or opportunities – to the benefit of investors. The ability to transfer information across jurisdictions without a prescriptive equivalency standard will create a more flexible and competitive marketplace for Canadian businesses, while maintaining the same level of rigour in protecting privacy that is in place internationally, allowing Canada to meet any equivalency standards.

Consent exemptions for business activities

Additional clarity and guidance on the scope of the activities in ss. 18(1) and (2) of the CPPA would be of assistance to our members. Businesses may collect information because it is "necessary to provide or deliver a product or service that the individual has requested from the organization". However, it is not clear whether a separate express consent would be required to use the information for a purpose that is indirectly related to the product or service being contracted for (for example, for marketing purposes, to provide the consumer with information about new products or services by the firm or an affiliate, not offered at the time of the original request), or whether a new express consent would be required. We are of the view that additional requests for consent from clients should not be required for these related activities. There is a risk that obtaining the client's express consent for every possible use of their information could lead to consent fatigue and increase regulatory burden without any corresponding increase in consumer protection.

Furthermore, information may not be strictly "necessary" to deliver investment management services but may be helpful to provide additional context that would help the asset manager to achieve the client's desired goals. For example, in some situations, properly assessing the suitability of an investment for a client involves more than simply collecting risk tolerance and investment knowledge details – additional information about the client may be germane to their financial situation, such as whether they have lifestyle choices or particular requirements that require funding in the future (for example the need to fund a child's special educational requirements such as music lessons or involvement in athletic pursuits, a desire to

travel in retirement or family responsibilities such as caring for an aging parent). Obtaining this additional information from a client should not require separate consent; although it may not be considered strictly "necessary", it is a cornerstone of the "Know-Your-Client" (**KYC**) principle and serves to improve the quality of the investment management services provided to clients.

Our members question whether s.18(1)(b) of the CPPA, which prevents an organization from relying on an exemption to the consent requirement because the information is used to "influence the individual's behaviour or decisions," would apply to investment management advice. In many situations, the asset manager is not just managing the client's money, they are helping them to identify and prioritize their goals, to ensure that they have adequate funds to meet those goals. Often, this means collecting information and making recommendations that go beyond what is strictly required to provide a basic level of service, but is absolutely crucial to ensuring the asset manager is acting in the best interests of the client. We do not believe that investment management should be considered to be "influencing" the client.

It is important to note that investors hire portfolio management firms to provide discretionary asset management services; unlike securities dealers, clients do not approve individual trades. The client relies on the portfolio manager's expertise and the fiduciary duty owed by the portfolio manager to the investor. It is critical that the portfolio manager collect necessary information about the client, referred to as KYC information. Registered individuals at the firm use their investment knowledge to determine the appropriate portfolio of investments that would best align with the client's investment needs, risk tolerance and investment goals. The firm then presents its determination about the appropriate investment approach to the client for them to accept by entering into an investment management agreement (**IMA**). In this way, portfolio managers use their expertise to provide recommendations for clients' investment paths. This could arguably be seen to be "influencing" the client's behaviour or decision, but we do not believe this should preclude firms relying on the exemption to the consent requirement for this reason. Additional clarity on this point, and specifically the meaning of the word "influence," would be helpful to our members.

Further, as discussed above, with respect to asset managers, we believe that information that is required to be collected by an organization by law or regulation (for identification, and under AML rules, for example) would fall under the consent exemptions in s. 18(2) of the CPPA because the activity is "necessary to provide or deliver a product or service that the individual has requested from the organization" and "carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk" (other exemptions under s. 18(2) may also apply). We note that the term "standard business practices" in the 2019 Consultation included purposes such as "using information for authentication purposes"; "risk

management"; and, "meeting regulatory requirements", which provided some clarity as to the ability to rely on these exemptions, and we believe that including them in the CPPA would help clarify the parameters of these exemptions.

If asset managers are not able to rely on these exemptions and were therefore required to change the type and volume of information that is collected from or provided to their clients, there would be significant deleterious consequences to their ability to serve their clients. The need to communicate with clients to collect or provide information more frequently not only adds burden and costs on asset managers, but also contributes to "consent fatigue" and information overload to clients, making both the information and the consent less meaningful. Additional guidance on these matters would significantly reduce the burden on asset managers and mitigate the risk of inadvertent breaches of the requirements.

Updating information and obtaining consent

We recommend that organizations should be permitted to rely on existing consents and current privacy practices, and that the new requirements should only be implemented on a prospective basis.[2] This would be a reasonable exception and would significantly reduce the risk of additional burden on asset managers and "consent fatigue" on clients.

As we noted in our September 2019 comment letter, most individuals do not respond to requests for updated information or consent from businesses without repeated follow-up and extensive outreach. PMAC's member firms have reported that initial requests for information typically garner very low response rates from investors. This is particularly the case where the investor has hired a portfolio manager for discretionary asset management and therefore are not usually in touch on a frequent basis. Delays in responding to requests for consent and/or the inability to obtain such consent in a timely fashion could negatively impact clients' investment portfolios.

For example, due to COVID-19, the federal government allowed RRIF investors to reduce their minimum withdrawal amounts by 25% in 2020. One of our members advised that they interrogated their system and sent out an email reminder to those RRIF clients who had not yet made a change to inform them that the option exists. Another example would be annual RRSP contribution reminders – a provider may analyze which clients have not made a RRSP contribution before the deadline and generate a list of clients to contact. This type of information-gathering and use happens on a regular basis and is in the clients' best interests. The result of any

[2] Note that amendments to National Instrument 31-103 – *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (known as the "Client-focused Reforms") coming into force in 2021 will require at least annual updates to Portfolio Manager clients' personal information, and that the information required to be collected will increase significantly in volume, thereby adding to the risk of information and consent "fatigue" for clients.

delays due to the need to obtain additional consents stands to hurt the investors that both PMAC's members and the Government are trying to benefit and protect.

As we have noted above, portfolio managers owe their clients a fiduciary duty of care. The presence of the fiduciary duty is very important in the context of how PMAC members are required to treat their clients. This elevated duty of care is also bolstered by the contractual arrangements between asset managers and their clients and the third-party service provider oversight obligation in National Instrument 31-103 – *Registration Requirements, Exemptions and Ongoing Registrant Obligations*, the primary regulation that governs the conduct of our members.

Automated decision-making

Our members also request additional clarity regarding an individual's right to receive an explanation about the use of an automated decision system as required under s. 63(3) of the CPPA. Investment decisions are frequently made based on automated processes, such as approved proprietary algorithms. There are many other types of decisions that may be made on an automated basis within the investment industry. For example, portfolio rebalancing may be required due to market volatility of the type experienced at the beginning of the COVID-19 pandemic or for other reasons. This rebalancing may be driven by automated decision-making.

The frequency and volume of such decisions would make it difficult for a firm to isolate a particular decision made on behalf of a particular client in order to give the client an explanation of the prediction, recommendation or decision. This is particularly problematic in the case of investors who have hired a portfolio manager to manage their investments on a discretionary basis – these clients have placed their trust in the asset manager, knowing they are contractually bound to comply with an IPS and subject to a fiduciary standard.

We therefore recommend that a materiality threshold be added to the right to an explanation under section 63(3) so that an explanation would only be required to be provided when an automated decision system makes a "significant contribution" to a prediction, recommendation or decision that could have a "material adverse" impact on the individual.

Additionally, disclosure of the details of such processes could involve confidential commercial information and intellectual property. In this case, it is our understanding that the information is not required to be provided in light of the exception in s. 71(7)(b) of the CPPA, but additional clarity on this point would be beneficial.

Further, many asset managers use third-party service providers to automate decision-making processes involving clients (for identification, investment decision-making, or other purposes). The asset manager may not have information about the

decision-making process of a third-party, and it is not clear whether they would be required to obtain such information and provide it to the individual. This may be especially problematic where the information is protected by a non-disclosure agreement or where the third-party refuses to provide the information (because it is confidential commercial information or for any other reason); it is not clear whether this scenario would be contemplated by the exception in s. 71(7)(b) of the CPPA.

For example, a firm may use a third-party system to generate an IPS for a client, which governs the investment parameters for the client's account. The IPS or investment projection is based on information about the client's investment knowledge, objectives, withdrawal schedule, risk tolerance, etc. The information is inputted into the service provider's software, which generates a report. The report or IPS is personalized and provided to the client for review in a "plain language" format and may be branded with the asset manager's logo. In this situation, the firm may not be aware of the details of how the service provider uses the information to generate the report, and the service provider may object to providing this commercially sensitive information. A lengthy detailed explanation of how such software works could be expensive to provide and likely would not be useful to the client.

Automated systems may also be used for AML and KYC verification. It is possible that an institution would not be permitted to or may decide not to accept a new client if they are unable to verify their identity (particularly in the fintech space). It may not be in the public interest to disclose information to an individual with respect to a decision made about them by such a verification system, but the exemptions to s. 63(3) in the CPPA do not appear to address this situation. Again, additional clarity on the requirement and any exceptions would be beneficial to PMAC members.

Privacy Management Program

Most asset managers already have robust privacy programs in place and provide information to clients with respect to information that is collected and the purposes for which the information is used. As noted above, firms are required to collect and keep records of information that is very likely to be sensitive to comply with regulations including securities law, AML requirements and under FATCA/CRS. Some members expressed concern with the requirement in s. 9(2) of the CPPA, to consider the "volume and sensitivity" of personal information under an organization's control. This is because existing systems may not be directed at these factors – smaller and less mature organizations may not have the ability to categorize such information (by using technology to "tag" or capture it, for example, and may treat all information collected to be "sensitive"). Tracing and de-identifying information may pose a significant challenge for these organizations. This is one example of the numerous changes that may be required within an organization to comply with the CPPA. Given the severe consequences of non-compliance, our members suggest that this type of

categorization should only be required on a go-forward basis. Alternatively, a staged implementation of the CPPA would be desirable, such that the aspects that may require changes to systems and technology have a longer timeframe to allow firms the ability to work towards compliance.

Right of disposal

This right as drafted is concerning as firms may need to retain information for appropriate purposes that are not captured by the existing exemptions (e.g. for fraud or security purposes, in anticipation of litigation, to comply with regulator expectations, etc.). We believe that additional clarity and/or additional exemptions will be required for firms to comply with regulatory requirements.

Definition of "de-identify"

Our members request additional clarity with respect to the right to de-identify; it is unclear what personal information would constitute de-identified data and what falls outside of the scope of the law. This creates uncertainty as to when organizations can rely on exceptions that require de-identified data (such as for internal research and development). There might be a need for additional carveouts to address scenarios where both de-identification and obtaining consent are impracticable and these carveouts should be considered. The requirement to use de-identified data in the context of prospective business transactions is also concerning to the extent that proposed transactions may require the exchange of identifiable data.

Regulatory burden

PMAC supports the codification of existing guidance to bring certainty and advance standards for the protection of privacy. However, the proposed changes will present a significant burden to firms, especially for smaller enterprises. We urge you to give firms time to implement any changes. Making significant changes to policies, procedures, practices, contacting clients to re-paper agreements and obtain necessary consent, and re-negotiating agreements with service providers or finding new service providers will take significant time, effort, and expense to implement. We suggest that a staged implementation over a 24 to 36-month period would be appropriate.

We also urge you to continue to provide resources to assist smaller firms in particular. For example, sample privacy policy documents that can be tailored to specific businesses, best practices, etc. This is especially the case for new requirements such as destroying or de-identifying data.

Procedural Fairness

Given the severity of the potential monetary penalties under the CPPA, our members wish to emphasize the need to ensure procedural fairness in decision-making by the Commissioner and the Personal Information and Data Protection Tribunal (**Tribunal**).

Members expressed concern that only one Tribunal member must have experience in the field of information and privacy law under s. 6(4) of the Tribunal Act. Information and privacy law is a very complex and nuanced area of the law. Considering the significant responsibilities of the Tribunal, and the sizeable monetary penalties it is able to impose, we are concerned that requiring only one member to have expertise in this are will not be sufficient. We would expect that every panel of the Tribunal include some members who are experts in the field. We are also of the view that Tribunal members must include lawyers familiar with the rules of evidence and principles of administrative law and justice, and at least one member of a panel should be a lawyer in good standing with their relevant law society and/or professional regulator.

We are also concerned with the provision in s. 15(2) of the Tribunal Act that the Tribunal is not bound by the legal or technical rules of evidence in conducting a hearing. We believe that the business of the Tribunal and the consequences of its findings are sufficiently serious for the Tribunal to be bound by rules of evidence, or at minimum that rules should be developed for the treatment of evidentiary material that comes before the Tribunal.

We also recommend that measures be included to ensure appropriate procedural fairness at the investigation and inquiry phases of a complaint.

Harmonization

PMAC is pleased to see that the CPPA approach to consent and transparency reflects much the same approach as those adopted under the General Data Protection Regulation (EU) (**GDPR**), as well as some privacy law in the United States. This harmonization is essential to maintaining Canada's equivalency standard in other jurisdictions and ensuring our international competitiveness.

PMAC members have expressed concern that the Quebec government is taking a more prescriptive and restrictive approach to privacy in Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information.* This approach risks limiting the ability of Quebec businesses to operate or engage service providers outside of the province and limiting businesses in other provinces from having clients that are resident in Quebec. This would present a significant hardship to PMAC members that operate nationally, threaten innovation and competition, and ultimately have a negative impact on the Canadian economy, without any evidence

that the more restrictive Quebec approach is required to sufficiently protect Canadians' privacy. In our comments to the Quebec government, we urged it to align its privacy legislation to the proposals in Bill C-11 to better harmonize requirements across Canada for the benefit of Canadians and Canadian businesses.

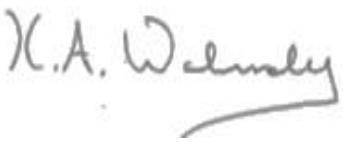
CONCLUSION

We are supportive of updating privacy legislation to improve clarity and consistency and advance privacy protection standards for all Canadians. Canadian privacy legislation should be robust, transparent, and aligned from coast to coast to protect individuals, support businesses, and ensure our competitiveness and attractiveness with trading partners. For asset managers, we agree that a reasonableness standard, exemptions to the consent requirements, and a principles-based framework are required to allow firms to tailor their policies and procedures to the type and quantity of information they collect, and to facilitate the use of personal information for the benefit of investors. Overall, we believe that Bill C-11 strikes the correct balance between protecting individuals' privacy rights while allowing asset managers to serve their clients effectively.

Thank you for the opportunity to respond to the draft legislation. If you have any questions regarding the comments set out above, please do not hesitate to contact Katie Walmsley at (416) 504-7018 or Victoria Paris at (416) 504-1118.

Yours truly,

PORTFOLIO MANAGEMENT ASSOCIATION OF CANADA



Katie Walmsley
President

Margaret Gunawan
Director
Chair of Industry, Regulation & Tax Committee,

Managing Director – Head of Canada Legal & Compliance
BlackRock Asset Management Canada Limited