VIA EMAIL: access.privacy@ontario.ca

September 3, 2021

Manager of Access and Privacy Strategy and Policy Unit
Ministry of Government and Consumer Services
Enterprise Recordkeeping, Access and Privacy Branch
134 Ian Macdonald Boulevard
Toronto, Ontario
M7A 2C5

Dear Minister Romano,

Re: *Modernizing Privacy in Ontario*

The Portfolio Management Association of Canada (**PMAC**) is pleased to have the opportunity to submit the following comments regarding the white paper, *Modernizing Privacy in Ontario* (**Consultation**). Although PMAC is supportive of efforts to enhance individual privacy rights, we are of the view that Ontario should await the outcome of federal efforts to modernize the *Personal Information Protection and Electronic Documents Act* (PIPEDA) (including the enactment of the *Digital Privacy Implementation Act* (**Bill C-11**)), to provide the appropriate flexibility of a harmonized national privacy framework.

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, and traditional as well as fully on-line or hybrid 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.

Most of our members operate across several provinces and territories and several of our firms are also international.

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).

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 will communicate privacy matters in a simple and straightforward manner. If Ontario adopts a new private sector privacy law, it must be harmonized with other laws (provincial and federal) and be interoperable to support innovation and ensure similar privacy protections for Ontarians.

Clients choose to invest their assets with portfolio managers for several 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 must do so in their best interests. 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 and harmonized 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.

National Instrument 31-103 – *Registration Requirements, Exemptions and Ongoing Registrant Obligations* (**NI 31-103**), the primary regulation that governs the conduct of our members, specifically includes client information-gathering and document retention provisions. 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.

Before providing our comments and recommendations on the proposals, we would like to thank the Minister for producing and publishing the white paper, which we found to be well written and easy to understand. It was tremendously helpful in providing additional context and rationale for the proposals and facilitated discussion among our members.

KEY RECOMMENDATIONS

PMAC's key recommendations are as follows:

- **Await the outcome of the federal efforts to modernize PIPEDA** (including Bill C-11) and focus efforts on advocacy at the federal level to ensure that any changes to privacy legislation are dealt with at a national level.

Ontario should only adopt privacy legislation as a last resort, for the reasons set out below.

- **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 experience and protections. Any changes should maintain adequacy status under international standards.

- **Adopt a principles-based approach to privacy that supports innovation while protecting individual privacy**. If Ontario decides that it is necessary to enact its own privacy legislation, the law should be robust, transparent, and clear. Ontario'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 Ontario decides to implement its own privacy legislation that differs from other Canadian private sector privacy laws, substantial changes may be needed for businesses to update their privacy programs. This will require significant time, resources, and capital. We therefore ask for a reasonable implementation period of at least 2 years to allow firms, and smaller businesses in particular, to adapt to any new regulatory requirements.

Harmonization

Before addressing the specific discussion questions in the Consultation, we wish to emphasize the critical importance of harmonizing privacy legislation across Canada. 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 Ontario and Canadian economies. We believe that Canadians should be entitled to similar privacy protections regardless of their jurisdiction of residence.

Although the Consultation notes several areas where Ontario believes that Bill C-11 does not go far enough in protecting individuals' privacy, 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 Ontario to await the enactment of the new federal privacy legislation before proceeding with provincial legislation. Canada may adopt in the

final legislation some of the recommendations suggested by the Office of the Privacy Commissioner of Canada and other stakeholders, thereby closing the perceived gaps identified in the Consultation. If Ontario were to adopt its own privacy legislation, even if it were aligned with the federal legislation, organizations would still be subject to a new and additional compliance regime in Ontario. This represents additional cost and regulatory burden to firms, without substantial added consumer protection. We therefore encourage Ontario to work with the federal government to eliminate any perceived gaps in Bill C-11. Ontario should only adopt a separate privacy regime if material gaps remain at the federal level, in which case we urge Ontario to seek alignment, where possible, to the federal legislation, to better harmonize requirements across Canada. PMAC 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*.

We noted in our response to the recent Federal consultation on Bill C-11 that PMAC was pleased to see that the proposed consent and transparency provisions reflect 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.

We have the following comments on the various discussion questions in the Consultation. We have set out each Consultation question to which we are responding for ease of refence.

Rights-based approach to privacy

- **Does the proposed preamble in this section include the right principles, reasons and values to guide the interpretation of a potential privacy bill?**

Members expressed concern with the implication in the first and second paragraphs of the preamble[1]. Recognizing privacy as a fundamental right will not necessarily achieve the correct balance with the legitimate need for organizations to collect and process personal information. Any move to a rights-based approach should align across Canadian privacy laws. In addition, the statements in the preamble that organizations are collecting "vast amounts" of personal information and "undermining the control" individuals have over their personal information are overstatements and imply that organizations are currently not taking steps to protect personal

[1] The paragraphs read: "Privacy is a foundational value in society. Every individual is entitled to a fundamental right to privacy and the protection of their personal information… Changes in technology have allowed organizations to easily collect vast amounts of personal information about individuals, often undermining the control that an individual has over their personal information."

information. We are of the view that the preamble would be more accurate and effective if the second paragraph – which serves no policy effect - was removed.

- **How should the concepts of personal information, and "sensitive" personal information, be defined in law?**

The Consultation does not state specifically which rights and/or obligations would attach to "sensitive" personal information. As a result, it is impossible to comment on the appropriateness of any definition.

We believe that a definition of "sensitive" information is not required and would be more appropriately set out in regulatory guidance. We do not believe that in all contexts financial information should be considered "sensitive," as there are other safeguards and regulatory requirements in place for asset managers sufficient to protect financial information. We believe that a risk-based approach is appropriate considering context, reasonability and risk of harm to the individual. We note the recent release of additional guidance from the Office of the Privacy Commissioner of Canada on what is considered to be sensitive information. Importantly, definitions, protections and permitted uses should be harmonized across jurisdictions. Failure to do so will result in confusion for individuals and cause undue burden for businesses.

- **Do the "fair and appropriate purposes" proposed in this paper provide adequate and clear accountability standards for organizations and service providers?**

We agree that a principles-based approach is preferable. A principles-based approach will allow organizations to tailor their practices to the particular needs of their businesses and to the expectations of their clients. However, it is not clear what purposes would be considered "appropriate" but not "fair". Given that Bill C-11 does not include a reference to purposes that are "fair", we would support harmonizing with Bill C-11 and limiting the standard to "appropriate". We do not believe that there is a sufficient consumer protection justification to deviate from Bill C-11 in this instance. The factors enumerated in (2) are sufficient to clarify what would be considered "appropriate".

- **How far should the data rights of erasure and mobility extend? Should they include all information an organization has about an individual, or only the information the individual provided?**

<u>Access and disposal</u>

We agree that individuals should have the ability to have their data transported and deleted, but that such rights must be limited by what is reasonable and practical and where it does not create an undue burden. Existing legislation already provides sufficient safeguards such that an additional disposal request right is not necessary.

These existing protections include organizational accountability for information collected and used, a requirement to retain the information for only as long as necessary to fulfill the intended purposes, and complaint mechanisms for consumers.

Organizations may have personal information about an individual stored in backup or legacy systems that are not readily accessible, where retrieval and disposal would present an inordinate burden. 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 regulatory expectations, records retention policies, etc.). Given the desire to implement a principles-based regulatory framework, any requirement to inform the individual of the information that exists and to dispose of the information on request should be subject to a reasonableness standard, rather than prescribing the specific circumstances where disposal is not required. We also distinguish between information about an individual as opposed to information obtained from the individual. If a disposal right is adopted, it should be limited to information collected from the consumer, as information about the individual is mostly derived or inferred by the organization.

We strongly believe that the proposed requirements with respect to disposal by a service provider are too broad. Specifically, section (b) "ensure that the service provider disposes of the information", is not a feasible standard. The contract governing the service arrangement may set out the service provider's disposal obligations, but organizations may have limited-to-no ability to ensure that information is, in fact, deleted. To impose this contractual obligation on service provided will require a vast number of contracts to be renegotiated which will necessitate additional time and resources. The most that organizations may be to able to agree to without changes to service provider contracts is to obtain a confirmation that the information has been disposed of, as suggested in (c). We therefore ask that Ontario remove proposed section (b) from any legislation.

Data mobility

Mobility of data is a laudable goal, but mobility frameworks vary from one organization to another, and implementation can be a significant burden for organizations, both large and small. Any requirements should be flexible and tailored to accommodate organizations of different sizes and capabilities, in an effort to better support the consumer. Implementation should be deferred until sector specific standards have been developed.

Data mobility should be limited to personal information collected directly from the individual (that is, to information that the individual has provided). In the asset management industry, clients may deal with multiple institutions of various sizes. It is desirable to have portability of information, but institutions should only be required to share the information necessary to achieve the stated purpose. In addition, the client may not wish to share all their information so a "one size fits all" approach will

not work. Additionally, the relevance of the information will be specific to each institution. For example, information provided by the individual could include "know-your-client" (**KYC**) information such as a person's individual investment goals, risk tolerance, and financial circumstances. Some such information may be the product of a firm's relationship with the client built over months or years and should not automatically be required to be transferred to another organization. Additionally, this type of information may be outdated and/or subject to human bias, as these determinations often involve the use of professional judgement. With respect to an assessment of a consumer's risk tolerance, for example, that risk tolerance is determined in the specific context of what the firm collecting the personal information offers its investors. Requiring the transfer of subjective information may do consumers a disservice.

Safe use of automated decision-making

- **Do the example provisions provided in this section offer adequate protection for Ontarians whose information is subject to ADS practices?**

In the asset management industry, automated decision-making has been implemented in multiple ways to provide increased access to investment advice at a lower cost, in a timely manner and with improved investment outcomes – these are examples of socially beneficial innovation in artificial intelligence. Such systems can be used to assist an investor in determining their risk profile, in collecting know your client information, in balancing portfolios according to the investor's goals, and in executing trades. We therefore support a balanced approach that provides protections where an automated decision may have a "significant" impact on an individual, while weighing these protections with the organization's ability to increase innovation and efficiencies relating to routine processes and activities.

Investment decisions under discretionary asset management services are frequently made alone or in conjunction with 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 investment portfolio rebalancing may be driven by automated decision-making.

The frequency and volume of automated decisions would make it difficult for a firm to isolate a particular decision made on behalf of a particular client and to determine if an automated process assisted with the decision, 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 Investment Policy Statement (**IPS**) and are subject to a fiduciary standard.

We therefore recommend that a materiality threshold be added to the right to an explanation 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 via explanations could involve confidential commercial information and intellectual property. In this case, an exception to the requirement to provide an explanation should be provided.

Further, many asset managers use third-party service providers to automate decision-making processes involving investors (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 third-party confidential commercial information or for any other reason such as the service contract does not impose any such obligations on the third-party service provider).

For example, a firm may use a third-party system to generate an IPS for a client. The IPS is the contract which governs the investment parameters for the client's account. The IPS or investment projection is based on information obtained from the client about the client's investment knowledge, objectives, withdrawal schedule, risk tolerance, etc. The client 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. An explanation of how such software works could be expensive to provide and, more importantly, would not likely be useful to the client.

Automated systems may also be used for Anti-Money Laundering and Anti-Terrorist Financing (**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). We also note that 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 in the case of an AML determination.

- **Does the proposed regulatory approach for ADS strike the right balance to enhance privacy protections, while enabling new forms of socially beneficial innovation in AI?**

The meaning of "socially beneficial" is not clear. The proposed provisions related to transparency (not exclusively as it relates to socially beneficial innovation in AI) are unique relative to other jurisdictions. This lack of harmonization may result in organizations choosing not to re-invest in such processes or technology if the resulting compliance burden is too high. This would be contrary to the Consultation's goal of "making Ontario the world's most advanced digital jurisdiction."

- **Should there be additional recordkeeping or traceability requirements to ensure that organizations remain accountable for their ADS practices?**

As noted in the Consultation, additional recordkeeping requirements will add substantial regulatory burden for organizations, and therefore should be limited to what is reasonable and linked to a clear regulatory purpose. In particular, additional detail with respect to traceability requirements is necessary to determine whether traceability is possible. The feasibility and potential burden of compliance cannot be assessed without additional clarity.

- **Are there additional requirements or protections that Ontario may consider related to the use of profiling?**

The distinction between "profiling" and "automated decision-making" is not entirely clear – these two concepts overlap. The definition of profiling is quite broad and should be clarified. We suggest it refer to "an individual's features, activities or attributes," as set out in the Consultation. If limits on profiling are to be introduced, these should be clearly set out in consideration of consumer risk and should be distinguished from other permissible forms of automated decision-making. Limits should not be so broad as to impede legitimate forms of automated decision-making but instead should be principles-based and risk-weighted.

Enhancing consent and other lawful uses of personal information

- **Does the sample list of "permitted categories" provide a sufficient set of authorities for the collection, use and disclosure of personal information? Are there any categories missing? Are there any categories that are too permissive?**

PMAC supports the proposed business activities list to facilitate the collection and use of personal information without an individual's consent or knowledge by firms under certain circumstances. We agree that an individual's knowledge or express consent

should not be required when transferring information to a service provider. We believe these provisions 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 supports the exemption to 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.

Our members question whether the prohibition under Business Activities section (b), 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 clients to identify and prioritize their goals and 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 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's decisions.

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 client. It is critical that the portfolio manager collect necessary information about the client, referred to as KYC information. Registered individuals at asset management firms 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 business activities exemption to consent requirement for this reason. Additional clarity on this point, and specifically the meaning of the word "influence," would be helpful to our members.

- **Consider the sample "business activities" provision provided above. Is it properly balanced to protect personal information while allowing businesses to conduct their operations? How should Ontario define the concept of "commercial risk"? Should "any other prescribed activity" be removed from the list of business activities?**

"Necessary" information

Additional clarity and guidance on the scope of the activities in (2) would be of assistance to our members. Businesses may collect and use 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 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 offered by the firm or an affiliate which were not offered at the time of the original request), or whether a new consent would be required for this related activity. 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 additional consent for every possible use of their personal information could lead to consent fatigue and increase regulatory burden without any corresponding increase in consumer protection.

Furthermore, collection of personal 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 may be germane to the client's 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 personal information from a client should not require separate consent; although it may not be considered strictly "necessary to provide or deliver a product or service", it is a cornerstone of the KYC principle and serves to improve the quality of the investment management services provided to clients.

Further, with respect to asset managers, we believe that personal 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 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", and is "authorized or required by law."

If asset managers are not able to rely on such exemptions and were therefore required to change the type and volume of personal 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 obtain consent 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.

Direct relationship

The Consultation notes that Ontario is proposing to omit an exemption where "obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual." We disagree that this provision would allow the collection and use of personal information without consent "on the basis of convenience or expedience". We believe that suitable limits could be imposed to allow such an exemption on principled grounds for legitimate business purposes.

There are situations where it is not possible or practical to obtain the consent of a person whose information is being collected or used, because they are not a party to the relationship. Such an exemption would be necessary for asset managers acting for third party beneficiaries of a trust or other arrangement, for instance. Effective as of December 31, 2021, securities laws will require firms to collect from clients personal information about a third-party Trusted Contact Person for older or vulnerable investors. This would include the name and contact information of a third-party, such as an emergency contact. Other examples where the asset manager would not have a direct relationship with the third-party individual include the collection and use of personal information about key employees or owners of a corporate client for KYC purposes, or the collection and use of personal information of recipients of e-transfers or wires who are not clients of the financial institution. For this reason, PMAC believes suitable limits need to be placed on this provision.

- **Are there any additional protections or requirements that Ontario should consider in respect of service providers?**

We agree that organizations should have the ability to disclose personal information to a service provider without consent of the individual. The ability to transfer personal 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.

However, we believe the service provider should be permitted to use the information to provide the services they are retained to provide. We agree that other uses should be held to the "appropriate" standard. We note that asset management firms are subject to third-party service provider oversight obligations in NI 31-103.

Moreover, organizations also frequently hire third-party service providers with the goal of protecting clients and their personal information. For example, cloud data providers that allow the safe storage of client data, companies that provide electronic signature capabilities to allow clients to be on-boarded remotely, companies that enable electronic delivery of investment statements, companies providing identify verification technology, etc. These companies are often vastly larger than the organization, and the organization has very little leverage to negotiate the terms of these standard service contracts.

Data transparency for Ontarians

- **Is the "privacy management program" requirement sufficient to ensure that organizations are accountable for the personal information they collect?**

We agree that an organization's privacy management program should be scalable to the size of the organization and we believe it should also be tailored to the nature of the business. Asset managers already have robust privacy programs in place and provide information to clients with respect to personal information that is collected and the purposes for which the personal information is used. As noted above, firms have a regulatory requirement to collect and retain records of information that is likely to be considered "sensitive" under securities laws, AML requirements and both the U.S. and international tax-reporting regimes, the Foreign Account Tax Compliance Act (**FATCA**) and/or the Common Reporting Standard (**CRS**).

Some members have expressed concern with the requirement to consider the "volume, nature 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 new provincial privacy legislation. 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 legislation 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.

Again, harmonization of requirements is essential so that organizations are not required to tailor their policies, procedures, and training to multiple regimes in various jurisdictions.

- **Are the sample provisions in this section sufficient to ensure that Ontarians understand the nature, purpose and consequences when an organization collects or uses their personal information?**

We agree that the listed information should be made "readily available". We generally prefer principles-based regulation and less prescriptive requirements. We agree that the sample provisions provide sufficient flexibility to allow organizations to provide information to consumers while limiting the risk of "information fatigue".

Regarding the information for consent to be valid, the requirement to communicate the "reasonably foreseeable consequences of the collection, use or disclosure of the personal information" (in s. 2(iv)) is very broad. Depending on the circumstances, it may be difficult to predict the consequences, and attempting to do so risks confusing the consumer. In this case, informing the consumer of the actual uses and disclosures of the personal information would likely be sufficient.

Obtaining consent

We recommend that organizations 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.

The result of delays in managing a client's assets due to the need to obtain additional consents stands to hurt the investors that both PMAC's members and Ontario are trying to benefit and protect.

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 the parties are not usually in touch on a frequent basis. Delays in responding to requests for consent and/or

[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.

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 Registered Retirement Income Fund (**RRIF**) account holders 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 Registered Retirement Savings Plan (**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 clients' best interests.

- **Should Ontario consider a mandatory requirement for "Privacy by Design" practices or "privacy impact assessments"? What kind of burden would this kind of requirement cause for organizations? How should Ontario balance the value of these requirements with this potential burden?**

We believe that such requirements impose a significant regulatory burden without a clear privacy benefit for consumers. Under current principles-based privacy legislation, organizations are already accountable for complying with all privacy requirements and for scaling their efforts to the sensitivity of the personal information involved, including the management of privacy risk. "Privacy by design" practices that default to the "highest level of confidentiality" (as proposed in Quebec for firms collecting information by electronic means) would impose a very high burden, without corresponding benefit. Firms may use multiple software platforms, and these can change frequently – the costs of implementing a higher standard may be significant, and this may not be necessary in terms of the risk to consumers. Any such requirements should be risk-based and subject to high materiality thresholds. The interpretation of thresholds is subjective – a reasonableness standard that considers the type of system and its uses, the costs involved in implementing and the risk of harm to consumers would be more appropriate. We note that GDPR only requires such assessments where a high degree of risk to individual freedom is identified.

The Consultation does not provide any detail of what a requirement for organizations to conduct a "privacy impact assessment" and/or to follow "privacy by design" principles would entail, and we are therefore unable to provide specific commentary. However, we urge Ontario to consider whether such requirements would provide sufficient consumer protection benefits to justify the substantial regulatory burden and costs that may be associated with such requirements. Any requirements should be harmonized across Canada and should be scalable to the nature of the business and the quantity, type and sensitivity of the personal information that is collected.

A fair, proportionate and supportive regulatory regime

- **Would certification programs and codes of practices be effective in proactively and collaboratively encouraging best practices in privacy protection?**

We agree that privacy practices should be industry-specific, and that best practices should be coordinated. However, certification programs should not be mandatory. Such programs can be costly and burdensome, especially for smaller organizations. Instead, these should be viewed as a tool that organizations can use to enhance their knowledge, improve their practices, and reduce uncertainty, if they so choose. It should be left to industry to develop codes of practices where this is viewed as necessary and appropriate.

- **Are administrative monetary penalties effective in encouraging compliance with privacy laws? Are the financial penalties set at an appropriate level?**

PMAC agrees that there may be instances in which greater financial consequences for organizations may incentivize compliance. We are in favour of rules supported by clear guidance on implementation and applicability, including effective and appropriate enforcement measures. We believe that the imposition of any penalties should be subject to similar to the procedural fairness principles available to organizations in Bill C-11. For example, any penalty should be subject to findings of misconduct and subject to a due diligence defence. Any penalty must also be aligned with other regulations so as not to add undue burden and cost to firms and investors, and to ensure procedural fairness. Increased fines and monetary administrative penalties may have the unintended consequence of stifling innovation and increasing legal and compliance costs to firms. These may be unnecessary as civil causes of action for negligence and privacy breaches already exist in Ontario common law.

Members are concerned that they may be subject to different enforcement provisions in various jurisdictions, and it is not clear how the different jurisdictions will interact or overlap with respect to enforcement matters and penalties. Given the potentially significant penalties for non-compliance, we would like to better understand how the provinces and the federal government will work together to ensure fairness when it comes to enforcement of privacy obligations.

We recommend multi-jurisdictional coordination of orders and penalties where organizations operate in multiple provinces. Without this, there is a risk of cumulative penalties that collectively may be unreasonable for an individual incident, or the risk of a series of disparate or contradicting orders that are challenging to implement.

- **Would the ability for the IPC to issue orders requiring organizations to offer assistance or compensate individuals be an effective tool to give individuals quicker resolutions to issues?**

We do not believe that it is the role of the IPC to determine whether individuals should be compensated. Many organizations already provide voluntary compensation regimes or services for impacted consumers. Any compensation process should be subject to appropriate procedural safeguards and evidentiary standards for organizations and consumers. We would expect that any such proceeding would be before a properly constituted administrative tribunal or court.

Supporting Ontario innovators

- **Would the clearer articulation of which privacy rules apply to de-identified information, as discussed in this section, encourage organizations to use de-identified information, and therefore reduce privacy risk?**

We agree that a framework for the use of de-identified information should be premised on a proportionate and risk-based approach. Encouraging the use of de-identified information for analytic uses would reduce privacy risk.

- **Would the inclusion of the concept of anonymized information, and clarifying that the privacy law would not apply to this information, encourage organizations to use anonymized information?**

We agree that exempting anonymized information from the Act would foster innovation, if appropriate safeguards are put in place to ensure that the information is truly anonymized.

CONCLUSION

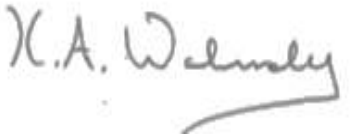
We are generally supportive of modernizing privacy legislation to improve clarity and consistency and advance privacy protection standards. We urge Ontario to await the outcome of Bill C-11 before deciding whether to enact provincial privacy legislation and, if legislation is to be enacted, what to include in any such legislation. 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 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.

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