The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

COMMENT LETTER

March 31, 2020

ICI Global Letter to Canadian Government on Proposed Overhaul of Data Privacy Legislation (pdf)

March 31, 2020 Sent electronically to charles.taillefer@canada.ca Mr. Charles Taillefer Director, Privacy and Data Protection Policy Directorate Marketplace Framework Policy Branch, Strategy and Innovation Policy Sector Innovation, Science and Economic Development Government of Canada RE: Proposals to Modernize the Personal Information Protection and Electronic Documents Act (PIPEDA) Dear Sir, ICI Global1 appreciates the opportunity to provide feedback on the Canadian government's proposals to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA), as set forth in the discussion paper "Strengthening Privacy for the Digital Age" (Discussion Paper).2 Because changes to data privacy laws can have a significant impact on our members' ability to serve investors in registered investment funds, we closely follow regulatory developments in this area. We support Canada's efforts to update its federal data privacy framework to further its policy aim of protecting investors' personal information while maintaining international competitiveness and predictability for businesses. From a process standpoint, we support the government taking the lead on any changes to PIPEDA and believe that any changes to guidance or practice from the Office of the Privacy Commissioner (OPC) should not front-run the federal legislative process. 1 ICI Global carries out the international work of the Investment Company Institute, the leading association representing regulated funds globally. ICI's membership includes regulated funds publicly offered to investors in jurisdictions worldwide, with total assets of US$32.9 trillion. ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of regulated investment funds, their managers, and investors. ICI Global has offices in London, Hong Kong, and Washington, DC. 2 Strengthening Privacy for the Digital Age: Proposals to modernize the Personal Information Protection and Electronic Documents Act, Innovation, Science and Economic Development (ISED) Canada, available at https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html. Mr. Charles Taillefer March 31, 2020 Page 2 of 9 Given the challenge of crafting a privacy law framework that achieves Canada's policy objectives without causing significant unintended consequences, we were pleased to see that the OPC determined not to change its 2009 policy position on transborder data flows.3 OPC's 2009 policy position provides that a transfer of data for processing does not require a customer's specific consent.4 This position allows global businesses, such as asset managers, to transfer data for processing to service their customers effectively and efficiently operate across multiple jurisdictions. The massive industry response to the OPC's initial consultation illustrates the need to craft PIPEDA amendments carefully in a manner that preserves the ability of global businesses to

continue servicing customers effectively and efficiently.5 We are pleased that, as Canada pursues reforms to its federal data privacy framework, it seeks to ensure that these reforms remain workable with multiple leading jurisdictions' data privacy frameworks.6 Many of our members operate in multiple jurisdictions and must manage numerous privacy requirements as they conduct a global business. Based on our members' experiences in dealing with data privacy laws in the United States and European Union, we offer for your consideration three recommendations: 1) Create exceptions for financial institutions' standard business activities; 2) Consider carefully the treatment of, and appropriate exemptions for, certain personal information of employees; and 3) Avoid conflicts with international privacy frameworks and other legal requirements. We discuss these recommendations in more detail below, and we look forward to providing more detailed stakeholder feedback on the text of any legislative amendments to PIPEDA. 3 Commissioner concludes consultation on transfers for processing, OPC (Sept. 23, 2019), available at https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/. 4 Guidelines for processing personal data across borders, Office of the Privacy Commissioner (January 2009), available at https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/. 5 "During its consultation, the Office received 87 submissions. Stakeholders, including industry representatives, raised concerns with respect to the position that consent may be required for transfers for processing. The vast majority took the view there was no requirement under the Personal Information Protection and Electronic Documents Act (PIPEDA) to seek consent for transfers for processing and that doing so would create enormous challenges for their business processes." See supra at note 3. 6 As the Discussion Paper describes, "[n]ext generation privacy and e-protection laws, specifically in the European Union but also in the United States, are impacting domestic policies and practices. There is a desire for an approach to personal information protection in the private sector that meets Canada's needs and remains interoperable with leading jurisdictions." Mr. Charles Taillefer March 31, 2020 Page 3 of 9 I. Create Exemptions for Financial Institutions' Standard Business Activities We support the Discussion Paper's proposal to provide certain alternatives or exceptions to consent to facilitate use of personal information by businesses under specific circumstances (for example, use of a consumer's personal information in connection with standard business practices). The Discussion Paper notes that "standard business practices" could capture purposes such as fulfilling a service; using information for authentication purposes; sharing information with third-party processors; risk management; or meeting regulatory requirements. The Discussion Paper poses the following questions on consent and transparency: 1) What are the benefits or risks of removing the requirement to obtain consent to process personal information for purposes that are considered to be standard business practices? 2) What activities should be captured by such a provision? Consent requirements, along with requirements that allow consumers to opt out of the sharing of their information, are an integral aspect of many data privacy laws. It is essential, however, that these consent requirements be tailored appropriately. Without a careful approach, consent requirements can impede a business's use of a consumer's personal information that is necessary for the business to provide goods or services that the consumer has requested. For example, requiring a consumer to consent to each incidence of use, or sharing, of their information with a financial institution's service provider would impede the ability to provide services to a consumer in a timely and efficient manner. Without a proper tailoring of the consent requirement, consumers would face a more cumbersome process and perhaps a more costly transaction. To avoid this potential outcome, consent should only be required for uses of consumers' information that are outside of standard business activities. Appropriate exceptions for standard business practices will ensure that financial institutions will be able to provide financial products and

services to consumers in a timely and efficient way. The United States is an example of a jurisdiction that has successfully addressed this need for exceptions when sharing consumer information for standard business practices. The US Congress enacted a comprehensive privacy law in 1999, Title V of the Gramm-Leach-Bliley Act (GLBA), which applies broadly to financial institutions. This law focuses on protecting consumers' privacy rights without impeding the ability to share consumers' non-public personal information (NPPI) to provide financial products and services to those consumers.7 7 See Gramm-Leach-Bliley Act, Pub. L. 106–102, 113 Stat. 1338, enacted November 12, 1999. SEC registrants subject to the GLBA are those that are "financial institutions" under the GLBA because they engage in "activities that are financial in nature" as defined in Section 4(k) of the Bank Holding Company Act of 1956 (BHCA), 12 U.S.C. § 1841, et seq. These registrants include funds (as an issuer of securities under Section 4(k)(4)(D)) of the BHCA); a fund's adviser (pursuant to Mr. Charles Taillefer March 31, 2020 Page 4 of 9 Title V of the GLBA requires a financial institution to adopt a privacy policy, provide the policy to its consumers in writing at the beginning of the financial institution's relationship with the consumer, and provide consumers the right to opt out of a financial institution's sharing of the consumer's NPPI with unaffiliated third parties under certain circumstances.8 Importantly, the GLBA includes exceptions that preclude the need for a financial institution to provide its consumer the right to opt out of the sharing of certain NPPI. These exceptions are designed to avoid impeding financial institutions' sharing of NPPI for legitimate business purposes. In particular, Title V of the GLBA permits a financial institution to share a consumer's NPPI in any of the following circumstances without providing the consumer the opportunity to opt-out and without the consent of the consumer:9 1) To carry out transactions; 2) To protect confidentiality of records; 3) To protect against fraud; 4) For risk control, dispute resolution, or customer inquiries; 5) To a customer's representative or someone with a legal or beneficial interest; 6) For insurance or compliance purposes; 7) As required by law; 8) To a consumer reporting agency; or 9) In connection with a business transaction. The full text of the GLBA exceptions is attached in Appendix A. These exceptions, individually and collectively, enable US financial institutions to service their consumers and conduct business without undue and unnecessary impediments while simultaneously protecting the privacy of consumers' NPPI. California, the only state in the United States to date that has adopted a comprehensive state data privacy law, included a carveout for data that is subject to the GLBA.10 Section 4(k)(4)(C) of the BHCA); a fund's underwriter or distributor (pursuant to Section 4(k)(4)(E) of the BHCA); and the fund's custodian (pursuant to Section 4(k)(4)(A) of the BHCA). 8 See Title V, Subtitle A of the GLBA, codified at 15 U.S.C. §§ 6801-6809. US law also limits the sharing of NPPI with affiliates for marketing purposes. These provisions were enacted after Title V. 9 See Section 502(e) of the GLBA. 10 See, e.g., Section 1798.145(e) of the California Civil Code, added by the California Consumer Privacy Act of 2018 (CCPA), which provides a carveout from most provisions of the CCPA for information subject to the GLBA (generally, the requirements of the CCPA will not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act). Mr. Charles Taillefer March 31, 2020 Page 5 of 9 Without these exceptions for standard business practices, or an opt-out framework like that used in Title V of the GLBA, consumers would need to respond to constant, burdensome requests for consent for sharing of their information in order to receive the financial products and services they have requested. Including exceptions such as those found in Title V of the GLBA for standard business practices would be in the best interest of consumers by preventing longer processing time as well as more cumbersome consumer engagement in connection with transactions. This type of approach also is consistent with the goals described in the Discussion Paper.11 Another important component of the standard business practice exception is an appropriate carveout for data collected from individuals in

the course of conducting business on behalf of their organization. In the fund industry, it is important to ensure appropriate exceptions for information that asset managers collect, in the ordinary course of business, from individuals who are acting as agents for institutional investors. For example, an asset manager may need to collect personal information for individuals who are authorized signatories for an institutional investor. Similarly, asset managers may need to collect information to satisfy legal obligations (i.e., Know Your Customer (KYC)/anti-money laundering (AML) obligations). Privacy laws should include appropriate carveouts that are carefully crafted to avoid sweeping in this type of data and creating significant and unnecessary compliance burdens. Other privacy laws have not appropriately tailored exceptions for personal information collected from an individual in their capacity as the agent of an organization. For example, the original text of the California Consumer Privacy Act of 2018 (CCPA) did not provide an exception for personal information collected by a business where it is communicating with an individual who is acting on behalf of another organization, even where the communication occurs solely within the context of a business transaction.12 The CCPA was later amended to provide companies a limited reprieve from complying with many of the requirements of the CCPA in the context of communications and transactions with agents of other companies, organizations, and government agencies (referred to as the business to business or B2B exception).13 This exclusion, however, expires at the beginning of 2021. 11 The Discussion Paper provides that '[i]n short, the goal is to respect individuals and their privacy by providing them with meaningful control without creating onerous or redundant restrictions for business" (emphasis added). 12 Among other rights, the CCPA allows consumers the right to receive information about the information that businesses collect about them, and to request that the business delete the personal information that the business has collected regarding the consumer. See, e.g., Sections 1798.100 and 1798.105 of California's Civil Code. The terms "consumer" and "personal information" are defined broadly in subsections (g) and (o) of Section 1798.140. 13 See subsection 1798.145(n) of California's Civil Code. Mr. Charles Taillefer March 31, 2020 Page 6 of 9 II. Carefully Consider Treatment of and Appropriate Exemptions for Certain Personal Information of Employees We also would urge particular caution regarding the treatment of employee information. Appropriate exceptions are needed to avoid significant and unnecessary burdens on employers and to preserve a company's ability to manage its workforce. The treatment of employee information affects both domestic businesses with only domestic employees as well global businesses with employees working in multiple jurisdictions. This area can present significant challenges and is fraught with unintended consequences. We note lessons from two jurisdictions that illustrate our concerns. In the General Data Protection Regulation (GDPR), the European Union did not provide an exception for employee information,14 and information about employees is considered personal data within the scope of the GDPR.15 This information commonly includes employee records or human resources information and further extends to anything the employer collects that contains the employee's personal data (e.g., emails). Employees, like all other "data subjects," have (among others) the right to access their personal information that the business holds, the right to correct errors, and a "right to be forgotten."16 These GDPR rights can create significant burdens in the employment context. For example, an employee or former employee could use the GDPR's right to access all personal data to compel a company to undertake an intense document identification, review, and production exercise, potentially requiring the company to hire legal counsel (and other service providers) to produce all emails and other documents that reference the individual. In this electronic age, this could mean thousands and thousands of documents (e.g., drafts of documents or emails to multiple recipients and replies). Because a company must bear the cost of providing access to this information at an individual's request, an employee or former employee could use this right in a manner different from the manner

intended— for example, to obtain information in advance of litigation or to pressure an employer into a settlement so that the employer does not have to go through the very expensive exercise of identifying, reviewing, and producing access to all of the individual's personal data. 14 See, e.g., Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), Key Definitions, What is personal data?, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general- data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. 15 Section (1) of Article 4 of the GDPR defines "personal data" and "data subject" ("'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"). Neither term includes a carveout for employees or employee information. 16 See Article 15 (Right of access by the data subject), Article 16 (Right to rectification), and Article 17 (Right to erasure ('right to be forgotten')) of the GDPR. These three provisions convey rights to "data subjects" generally, and do not include a carveout for employee information. Mr. Charles Taillefer March 31, 2020 Page 7 of 9 The right to be forgotten also can present significant challenges and burdens, for example, when requested by a former employee whose name appears throughout documents, emails, and work product. These challenges compound in a circumstance where an individual has been employed by a company for a lengthy period of time. Under the GDPR, employers also struggle with uncertainty around identifying legal bases for using employees' personal data. Employers must rely on an employee's consent if they cannot identify another legal basis for using the employee's personal data. The requirements for valid consent under the GDPR are very stringent, however, and the validity of consent within the employment relationship can be challenged. Legislation at the national (Member State) level can provide additional legal routes to handling the data, but these routes can be very limited.17 This lack of certainty for employers subject to the GDPR is deeply problematic given the potentially significant monetary consequences of violations.18 The GDPR's application to employees' emergency contact information similarly illustrates the need for tailored exceptions. The GDPR applies to personal information collected for employees' emergency contacts and can require employers to provide a GDPR notice to the emergency contact, creating unnecessary compliance challenges without addressing the government's intended policy concerns.19 California's privacy legislation raised similar issues with employee information.20 The originally enacted text of the CCPA applied in full to personal information collected from employees, job applicants, and other personnel. The California legislature adopted a temporary fix to the CCPA that limits a business's CCPA obligations in relation to personal information the business collects about a person in the course of the person acting as a job applicant or an employee, owner, director, officer, medical staff member, or contractor of that business. The result is that businesses are required to deliver a short-form 17 Article 6 (Lawfulness of processing) of the GDPR provides that obtaining consent from the data subject is one of six circumstances under which data legally may be processed. Article 88 of the GDPR addresses processing in the context of employment and allows EU member states to provide for more specific rules to ensure the protection of employee rights and freedoms with respect to the processing of employees' personal data in the employment context. These provisions appear to contemplate more tailored provisions rather than broad carveouts. For instance, the UK's Data Protection Act 2018 accordingly makes further provision around the processing of "special category" (e.g., health-related) personal data regarding employees, outside of the consent basis for processing, in certain circumstances. 18 While not necessarily related to employee information, there have already been

significant fines imposed under the GDPR. For example, the French Supervisory Authority imposed a €50,000,000 fine on Google; the UK's Information Commissioner's Office imposed a £183.4 million fine on British Airways and a £99.2 million fine on Marriott for data breach-related violations. 19 This information is excepted in jurisdictions where employers are legally required to collect emergency contact information from employees. The exception does not apply, however, in jurisdictions where this is not legally required, although there has been some guidance regarding emergency contact information collected in the case of a hospital admitting patients. 20 See Section 1798.145(h)(1)(A-C) of the California Civil Code, added by amendments to the California Consumer Privacy Act of 2018 (CCPA), signed into law on October 11, 2019. Mr. Charles Taillefer March 31, 2020 Page 8 of 9 privacy notice to their employees and other personnel, and to job applicants, prior to January 1, 2021; however, such businesses are not required to comply with all of the requirements of the CCPA. Once the temporary reprieve expires, however, the CCPA will apply fully to information employers collect related to job applications, employment contracts, performance reviews, payroll processing, and benefits administration. California legislators and businesses with California-resident personnel continue to struggle with these issues. In addition to including appropriate exclusions for certain uses of data by employers, it is essential that any reforms to Canada's law preserve and accommodate a business's ability to transfer employee information within or outside of Canada where necessary for the business to fulfill its regulatory and legal obligations as an employer, provide benefits to its employees, or otherwise carry on its business activities. For example, many global businesses with activities in Canada may administer their employment obligations and provide benefits to their employees from administrative offices outside of Canada. Some companies hire global service providers to assist with payroll processing, including the processing of any deductions at source (i.e., federal and provincial income taxes, employment insurance, and Canada Pension Plan or equivalent contributions). In some financial services companies, certain employee information (including information collected for compliance regarding personal trading approvals) must be stored in a central database to be accessed by employees in various offices globally. Beyond human resource purposes, there may be business reasons for employee information to be transferred across borders (for example, cross-border project teams or employees who move among different countries). In addition, in light of the increasing importance of inclusion and diversity at organizations, it may be necessary for multinational organizations to aggregate employee information from various jurisdictions for internal inclusion and diversity initiatives as well as for responding to regulatory or client inquiries regarding diversity at the organization. III. Avoid Conflicts with International Privacy Frameworks and Other Legal Requirements We support Canada's objective of preserving the free flow of information across borders while maintaining meaningful privacy protection. As stated in the Discussion Paper, "[p]romoting global interoperability of privacy frameworks is a key foundation of Canada's approach to privacy." The registered investment fund industry operates in a global environment where cross-border information flows, including transfers of personal data, are a fundamental element of providing financial services to fund investors. We, therefore, greatly appreciate Canada's goal of interoperability, and we encourage the Canadian government to help ensure its data privacy laws do not conflict with other key jurisdictions, such as the United States and European Union. A sensible and strong approach that also works well with other jurisdictions' frameworks (e.g., the GDPR) will help prevent increased costs and disruptions and is vital Mr. Charles Taillefer March 31, 2020 Page 9 of 9 for both Canadian businesses that conduct business across borders as well as businesses that are not Canada-headquartered but that do business in Canada. Choosing a flexible framework instead of an overly prescriptive framework will help ensure interoperability with other legal requirements. The use of data has become woven into virtually every aspect of modern

business, and it is impossible to foresee every manner in which a privacy law may conflict with other legal requirements. Ideally, reforms will be able to consider and address all needed exceptions. Even with the best efforts, however, there are likely to be unforeseen conflicts. We also urge Canada to consider its privacy laws in light of its other legal requirements and avoid any potential conflicts. As one example, our members experienced unforeseen conflicts in their efforts to comply with both the GDPR and anti-money laundering (AML) requirements. Financial institutions' efforts to comply with AML requirements necessarily involve detailed reviews and sharing of personal data. The GDPR failed, however, to take into account how its provisions would impact legal requirements relating to AML efforts in various jurisdictions. Financial institutions continue to have concerns about managing the GDPR's privacy protections and their AML obligations, including identification of customers during onboarding and due diligence on new customers.21 This example highlights the need for a framework that has the flexibility to ensure interoperability and avoid conflicts with other legal requirements. * * * * * We appreciate your consideration of the points we have raised in this letter. If you have any questions or would like additional information, please contact me (patrice@ici.org or +44-207-961-0833) or Jennifer Choi, Chief Counsel, ICI Global (jennifer.choi@ici.org or 1-202-326-5876). Sincerely, /s/Patrice Bergé-Vincent Patrice Bergé-Vincent Managing Director 21 See, e.g., Sharon Cohen Levin and Franca Harris Gutierrez, WilmerHale, Implications of the E.U. General Data Privacy Regulation for U.S. Anti-Money Laundering and Economic Sanctions Compliance, Chapter 5 of the International Comparative Legal Guide to Anti-Money Laundering 2018, 1st Edition, available at https://www.wilmerhale.com/en/insights/publications/20180621-implications-of-the-eu-general-data-privacy-regulation- for-us-anti-money-laundering-and-economic-sanctions-compliance. A-1 Appendix A Section 502(e) of the GLBA: Exceptions (e) GENERAL EXCEPTIONS.—Subsections (a) and (b) shall not prohibit the disclosure of nonpublic personal information— (1) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with— (A) servicing or processing a financial product or service requested or authorized by the consumer; (B) maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or (C) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer; (2) with the consent or at the direction of the consumer; (3) (A) to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein; (B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (C) for required institutional risk control, or for resolving customer disputes or inquiries; (D) to persons holding a legal or beneficial interest relating to the consumer; or (E) to persons acting in a fiduciary or representative capacity on behalf of the consumer; (4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors; (5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury with respect to subchapter II of chapter 53 of title 31, United States Code, and chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951–1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety; (6) (A) to a consumer reporting agency in accordance with the Fair Credit Reporting Act, or (B) from a consumer report reported by a consumer reporting agency; A-2 (7) in connection

with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; or (8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.
