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

701 West Georgia Street | Suite 1500
Vancouver, BC | V7Y 1C6
604.637.1677 | www.iiac.ca

www.iiac.ca

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

November 7, 2019
Charles Taillefer
Director, Privacy and Data Protection Policy Directorate
Innovation, Science and Economic Development ("ISED")
Charles.taillefer@canada.ca

Dear Mr. Taillefer:

Re: Proposals to Modernize the Personal Information Protection and Electronic Documents Act (the "Proposals")

The Investment Industry Association of Canada ("IIAC or the Association") appreciates the opportunity to comment on the Proposals.

We are pleased that ISED is taking steps to conduct a thoughtful and complete consultation involving industry and the public, in order to ascertain the way in which privacy regulation should evolve along with the changing technological landscape.

The IIAC is the national association representing 118 investment dealer firms on securities regulation and public policy. Our members are the key intermediaries in Canadian capital markets, accounting for the vast majority of financial advisory services for individual investors, and securities trading and underwriting in public and private markets for governments and corporations.

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

As noted in the consultation paper, the digital revolution has had and will continue to have an enormous impact on daily life. As such, the regulation of data use will have far reaching implications into the way in which business is conducted, with impacts on foundational business decisions relating to whether the cost of serving clients in a meaningful and personalized manner is feasible, given the regulatory structures that may be set up to protect their data. It is, therefore, critical that proposed regulation be structured to account for the way in which different industries use technology and data, allowing for

best practices among such industries to develop, rather than imposing a one-size fits all approach to all industries.

Industry Background

The evolution in technology has advanced all elements of the investment industry, from the back-office operations to the client experience. Investors now benefit from digitization, from the opening of an account, to asset allocation, trading securities, monitoring portfolio performance, financial planning and ensuring contact with their advisor takes place at key points in time. The vast amount of information and analytical capacity leverages the skills of advisors and investment managers to the benefit of their clients and provides investors with increased access and control over the information they receive, enabling them to better understand and direct their financial decisions.

In order to protect this critical data, investment dealers have developed robust data protection processes and safeguards within their firms, and in their interaction with third party processors. The industry has also worked closely with its regulator, the Investment Industry Regulatory Organization of Canada ("IIROC") to ensure clients benefit from appropriate protection of their data.

Introduction

We are pleased that the Proposals document acknowledges that the regulatory framework must strike an appropriate balance between providing individuals with meaningful control of their data, without creating onerous or redundant restrictions for business. We also agree that the framework should encourage responsible innovation on the part of organizations, and ensure an enhanced, reasoned enforcement model.

Given the importance of data in developing new and improved products and services, and the ever-increasing ways in which this data is collected and utilized, it is critical to ensure individuals have relevant information about how their data is being used and disclosed, while also ensuring that the collection and use of such data is not subject to unnecessary barriers that would impede innovation and development of beneficial products and services.

Part 1: Enhancing individual's control

A. Consent

Although the recent decision of the Office of the Privacy Commissioner has acknowledged the difficulties posed by obtaining specific consent prior to collecting, using or disclosing individuals' personal information, it appears that a consent-based model remains a cornerstone of the Proposals. Given the vast amount of data that is collected and used in increasingly novel and unanticipated ways as technology evolves, the principle of obtaining specific and detailed consent for each use of data that may be involved in the provision of a product or service has become increasingly unworkable and ineffective.

For instance, as the provision of personal data occurs at virtually every level of commercial activity, requiring individuals to provide consent for all of the interactions and usages imposes an unrealistic burden on the individual to read, understand and sign off on lengthy and sometimes complex privacy policies that will vary as between firms and industries.

Rather than requiring a more stringent consent regime, we recommend that the focus be on disclosure, i.e. that organizations provide plain language disclosure of how they use data in respect of carrying out their business activities.

Where consent may be required for the collection use or disclosure of personal information, we agree that consent should not be disclosed in the "fine print" and should be prominently presented within the contract or account opening documentation.

Firms are ultimately held accountable for the use of client information, in accordance with privacy regulatory requirements. The accountability principle in PIPEDA is a key driver of privacy compliance by organizations. Requiring additional consents from individual clients does not advance the fundamental objective of protection of client data, or give clients additional options for data handling. Where clients provide additional express consent, it may, in fact, shift some of the responsibility to clients, which could erode the concept of accountability for data that is currently at the heart of our privacy regime, and also that of the GDPR. It could also arguably shift the user's accountability to the "consenting" client and mitigate available damages should an issue arise as a result of the transfer of data. If the diminution of accountability and mitigation of damages result, that works against consumer interests, contrary to the objective and philosophy of the regulation.

The number of express consent requests and accompanying disclosure is likely to be overwhelming and annoying for individuals, who may ignore these requests for consent to their detriment. It may also provide an opportunity for cyber criminals to use the proliferation of consent requests to plant malware and perpetrate cyber-crime. This has occurred in Europe, where cyber criminals have used provisions of the GDPR to overwhelm data custodians with demands for disclosure of personal data.

In a data driven economy, requiring individual consent for data processing where the data is to be used in the ordinary course of providing the requested service will not provide additional security for individuals. Individual consent will not impact the security standards and data protection measures established by organizations that hold individuals' personal information. We support the creation of exceptions to consent for data processing which includes common uses of personal information for the provision of standard business activities that the individual is purchasing / obtaining.

In addition, the accelerating pace of technology means that consent provided at one point in time may have to be refreshed on an ongoing basis as technology evolves to allow for the same data to be used to provide an enhanced version of the contracted for services to the consumer (eg: analytics could more accurately provide better tailored investment advice based on the individual's data profile) Continually refreshing consent is not operationally feasible, and would also not provide additional data security for the individual.

Rather than relying on consent, regulators should emphasize and enforce the accountability principle, which underpins PIPEDA, to ensure that companies using personal data employ appropriate security for personal information.

We agree, however, that obtaining specific consent is important to transparency and accountability where individual data is to be used in a manner that is not integral to the provision of services for which the individual has contracted, for example, where data is being provided to third parties that are not involved in the provision of such services.

Where consent is required, it should be clear that only the information required as the basis for meaningful consent is to be provided. This means that the disclosure should be concise and must provide the opportunity for individuals to actually make a meaningful and informed decision, realizing that not providing consent may result in them not being able to obtain the desired service. The existing practice of notifying individuals of the purposes for collection, use or disclosure, and the types of personal information, at the time the information is collected, is sufficient to achieve transparency and allow for choice.

We do not believe sensitive personal information should be defined, as it is likely to be contextual, based on other information collected at that time or later. Defining sensitive personal information and adding additional protections would increase the burden without providing meaningful additional protections, particularly where the information is required to deliver the desired service. Again, the concept of accountability should be relied upon to ensure data security.

In addition, in respect of de-identified information, we believe there should be an exemption from the consent requirement for the use and disclosure of such information. In order to address situations where information is re-identified, we recommend reliance on the accountability principle, such that firms would have to establish that they followed appropriate standards in de-identifying the data.

For further background on our views regarding consent, we include our submission to the Office of the Privacy Commissioner, relating to the Consultation on transborder dataflows.

B. Data Mobility

The IIAC has some questions and concerns in respect of the Proposal to provide an explicit right for individuals to direct that their personal information be moved from one organization to another in a standardized digital format, where such a format exists. We support the principle of data mobility as a means to assist individuals in controlling their data, and an efficient means for companies to manage consumer information. However, the data to be subject to these provisions must be clearly and narrowly defined in order to prevent confusion, inappropriate disclosure, and operational feasibility. For instance, it should be simple to move a subset of information to another organization where not all of the consumer information held at a firm is relevant or appropriate for another organization to possess.

A possible unintended effect of data mobility that is not confined to specific and required information, may be to multiply the number of databases of information containing information about individuals,

rather than limiting them. Where recipient organizations use the information for different purposes, they may hold information that is not required for their business relationship without obtaining meaningful consent.

We recommend that the categories of data to be subject to mobility be clearly defined, so that only the appropriate and relevant data can be transferred between organizations. It should only include data provided by the individual, and not derived or third-party information. We are concerned that derived or third-party information may contain inaccurate, sensitive or other information that the individual may not wish to have shared. This would also introduce an increased liability risk to transferring organizations.

The data mobility provisions should also be contingent on organizations having appropriate technical standards covering data compatibility, authentication, security and other relevant controls. The timeline to mandate data mobility must take into consideration the time required to develop industry standards. It should also permit small business to opt out, in the event that the required standards pose a disproportionate burden for them to adopt. The regulation should also provide a safe harbor for the parties that are disclosing the data, to limit liability for acts or omissions of the recipient organization.

It is also important that the data that is subject to data mobility requirements be limited, and must not be equivalent to those available under the access provisions of PIPEDA. The scope of the information available for access under PIPEDA is very broad, and it would be impractical to create a standard digitized infrastructure and framework to allow for data mobility. In addition, much of this information is data that is not specifically provided by the individual, rather it is derived from a combination of individual data along with its interaction with collective data, regulations and institutional policies.

From a practical standpoint, the data subject to mobility requirements should be differentiated by industry. For instance, individual data provided to financial firms should only be sharable amongst other financial firms, and not, for instance, with health care providers. By categorizing the data, and limiting its mobility in this manner, the likelihood of inappropriate data leakage is minimized. In addition, the appropriate data sets, standards and formats would be more easily standardized within industry categories, as similar programs and protocols already exist to allow organizations to communicate and share data with each other. It is impractical to impose similar technology standards, protocols and formats across industries where data is collected, stored and used in very different ways and for very different purposes.

C. Online Reputation

While we agree that individuals should have some measure of control over their online reputation, we are concerned that the Proposals extend beyond concerns about youth and social media, and introduce significant operational burdens for industries that do not publicly disclose the personal information provided by their clients.

For instance, the investment industry collects a significant amount of data about its clients, in order to provide high value investment, financial planning and trading services, targeted specifically to their circumstances. This information is not made public, and is used/shared only within the firm and the third-party processors required to provide the contracted services.

It should also be noted that the self-regulatory rules governing investment professionals have prescriptive retention and deletion policies that were developed to specifically address the way in which the industry operates and the expectations of clients. The Proposals would introduce prescriptive measures that may conflict with certain of the existing industry provisions, and would also create significant compliance challenges in respect of data that is used in different ways within the firm, and shared with various processors to deliver a variety of services within the firm (eg, trading, financial planning, tax planning, retirement savings).

We recommend the Proposals be targeted to organizations and platforms that provide online public access to information about individuals, rather than provisions that apply to businesses that do not have an impact on an individual's online reputation.

Enabling responsible innovation

A. Enabling data trusts for enhanced data sharing

We support the development of data trusts as a means to pursue responsible innovation. The element of entrusting this data to third parties that have enhanced technical and governance controls is an essential part of the Proposal. We recommend that data trusts be restricted to using de-identified information, as this would help alleviate privacy concerns and operational obstacles, where, as proposed, such information was not subject to consent requirements.

B. Self-regulation and technical standards

The IIAC agrees the use of codes, standards and certification schemes are useful in improving regulatory agility and supporting responsible innovation. They also provide a measure of consistency and predictability in dealing with other jurisdictions, who look to these standards as a means of assuring that organizations can conduct cross jurisdiction business (such as with GDPR jurisdictions) without imposing additional requirements.

However, given the differences in size, operations, and use of data in different organizations, it is critical that the codes, standards and certifications are not developed as a "one size fits all" model. Rather, they should be flexible, to accommodate the specific data stored and the way in which data is used in an organization. It is important that, in order to be relevant and operationally practical, the industries that would be using these codes, standards and certification schemes be involved in the development of the protocols and standards.

The codes and certifications should also be voluntary, as they may not be applicable or practical for all organizations to enact. In this way, those handling a higher volume of personal information may be incentivized to comply with the relevant codes.

We believe the codes and certifications should be administered by a third-party certification body, qualified to undertake the appropriate oversight and review, subject to oversight by the Standards Council of Canada, rather than the OPC or other relevant privacy regulator.

We also recommend that the use of such codes and certifications be recognized in PIPEDA, such that compliance would be taken into account in ascertaining appropriate remedies should a non-compliance incident occur.

Enhancing Enforcement and Oversight

A. Education / Outreach

We agree that it is appropriate for the Privacy Commissioners to have an education and awareness mandate and provide guidance on complex matters covered by PIPEDA. We also believe it is appropriate to undertake research to allow for greater clarity for industry on emerging issues and in furtherance of policy development.

B. Investigation and Audit

We agree that it is appropriate to grant the Commissioner increased discretion in determining whether to investigate a complaint or discontinue an investigation. This will allow the Commissioner to focus on substantive and problematic issues. As noted above, we support the consideration of adherence to standards, certification or codes of practice in the determination of the Commissioner to investigate, and establish remedies.

We do not support providing the OPC with the authority to commence audits or periodically review an organization's adherence to a certification scheme. As noted above, we believe the certification schemes should be non-mandatory and administered by an independent third-party subject to oversight by the Standards Council of Canada, which would obviate the need for OPC to be granted new authority under PIPEDA to audit for compliance with such standards.

We are concerned that granting order-making and fining powers under PIPEDA may be contrary to the principles of fairness, in that the privacy regulator may be advocating for the complainant while acting as the arbiter. Should such powers be granted, it is important to create due process safeguards relating to evidence, ability to respond (with counsel if required), and an appeal process with independent panel members reviewing the regulatory decisions, prior to any published notice of violation.

We also strongly oppose adding statutory damages to PIPEDA. To support a fair system, each matter must be reviewed on its merits, assisting all relevant factors, rather than relying on pre-established punitive measures. We are concerned that this would create an environment conducive to the launching of opportunistic class action claims, which would divert industry and regulatory resources.

Areas of Ongoing Assessment

We agree that PIPEDA should maintain its principles-based and technology-neutral approach, allowing it to evolve with technology without requiring ongoing amendments. In addition, it is important that PIPEDA continue to be based on the accountability principle to avoid complex, prescriptive requirements that result in regulatory loopholes and the need to constantly update the regulation to keep up with new developments.

The accountability principle should, however, include clear requirements for accountability for processors and other third parties that use, store or otherwise come into contact with the data.

Industry Input

Thank you for considering our comments. We would be pleased to meet with you, and other appropriate individuals responsible for developing the Proposals to provide further input on the key considerations in data regulation for the financial industry. We will be in touch to arrange a meeting at a convenient time. In the meantime, if you have any questions, please don't hesitate to contact me.

Yours sincerely,

Susan Copland