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

IIAC LETTER

Data Privacy in the Investment Industry
Why Firms Need to Pay Attention

BACKGROUND

The financial industry has long been the guardian of individuals' most sensitive and valuable information. The manner in which this information is used and stored has undergone a sea-change in the past two decades. As information storage evolved from file cabinets to servers to the cloud, so too have the opportunities for data use and misuse. These abuses, and the growth of the technology fueling the information-based economy, provided the impetus for early regulation designed to manage the use and protection of personal information.

In 2000, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") was enacted in Canada, to "alleviate consumer concerns about privacy and to allow Canada's business community to compete in the global digital economy" [1] and to build trust in electronic commerce. Within 3 years, Alberta, British Columbia and Quebec enacted similar legislation covering certain activities taking place exclusively in their jurisdictions.[2]

Since then, new data sources such as social media platforms, search histories, online surveys and the publication of other sources of individuals' online information and activity have provided data repositories that can and are often used in combination with data provided by individuals and enhanced by the use of artificial intelligence, to create detailed profiles of individuals, often without their knowledge or consent. This information, in turn can be sold and used by entities for a variety of purposes, without a person's consent, and in ways which could be contrary to their interests[3].

As the digitization and use of information has expanded, policies and processes to safeguard and manage the data have not been consistently developed, implemented and regulated alongside the increased analytical and storage capability. Without a rigorous data governance framework, companies can easily lose control of how they manage information, leading in some cases to inappropriate uses of data and susceptibility to cybercrime.

In recent years, several high-profile breaches of personal data elevated the issue to the forefront, leading to public demands for regulation that ensure organizations are accountable for the way in

---

[1] From Industry Canada's website: Privacy for Business, Electronic Commerce in Canada
[2] PIPEDA defers to such provincial regulation, when it is deemed that it the provisions are substantially the same as PIPEDA.
[3] For example, information may be used to create and share profiles of individuals, which would in turn be used for benign functions such as marketing, but also potentially to target people (possibly to influence them or deny services) based on their political views, religion, sexual orientation or other characteristics.

which they collect, use, and protect an individual's personal information. This has triggered a new round of regulatory activity to address the challenges arising from the rapidly evolving and ubiquitous use of technology. These changes in data protection regulation exist along a continuum from supplementary guidance and best practices under PIPEDA in Canada, to new, more prescriptive laws in Europe and California that include binding obligations, enforcement mechanisms and monetary penalties for non-compliance.[4]

DATA PRIVACY AND THE FINANCIAL INDUSTRY

The stewardship of personal information is particularly important for the financial industry. Financial institutions hold some of their clients' most sensitive personal information, much of which is potentially commercially lucrative for legitimate and criminal purposes.

Aside from the obvious financial information such as account numbers, balances, investment account and trading data, in order to provide comprehensive financial advice, firms hold identification documents, information on clients' family, health, education, goals, work history, consumer activity and other confidential and sensitive information. Some of this information may be so sensitive that it is not even shared with other family members. As such, it is critical that this information not only be protected from cyber criminals, but that it also not be used or processed in a manner for which it was not intended by the client.

This is where it gets tricky. As technology evolves, the collection and use of information has come to provide beneficial insights and services that were not anticipated or imagined at the time the data was collected. Given that the technology is constantly evolving, and the processing takes place behind the scenes, informing the client and obtaining consent for the use of their information becomes wholly impractical as processing capability and new products and services that use this data emerge.

INTERNATIONAL LEGISLATIVE RESPONSE

The emergence of cybercrime, identity theft and other inappropriate uses of personal information prompted governments to respond by re-examining their privacy regulation. The most significant and comprehensive regulatory initiative to date is the General Data Protection Regime, ("GDPR") enacted by the European Union in 2016. This wide-ranging regulation has provisions that apply to other countries doing business in Europe, and has been a catalyst and template for many other countries and states to create or update their own privacy laws.

The GDPR contains a number of principles that have been adopted or proposed in privacy regulation by other jurisdictions, including Canada. Some of these common principles include individuals' rights in respect of their personal information. These rights include an individual's right to:

---

[4] Most notably, two data protection acts, Europe's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") have introduced new significant obligations, enforcement provisions and penalties. Many other international jurisdictions are using these regulations as templates for their own new privacy initiatives.

- consent to the use and processing of their data;
- object to automated decision making using their data;
- access their data held by an organization;
- rectification of any errors in their data;
- portability of their data for transfer between companies;
- deletion of their data; and
- be informed about how their data is used.

In addition, GDPR articulated several principles that must be considered when collecting and using information, including:

- data minimization (collecting as little data as possible to achieve the objective);
- privacy impact analysis (ensure the impacts of using the data are understood and justified);
- purpose limitation (the reason for processing personal data must be clearly established and indicated when the data is collected); and
- privacy by design (firms must build privacy protection into their systems and ensure that data protection is safeguarded in the system's standard settings).

Enacting these rights and principles have technological and operational implications. Certain of these rights, such as the right to consent and data portability, have been criticized as impractical or impossible to fully operationalize, and also create other privacy issues that can potentially undermine the objective of the regulation.

An over-arching requirement for consent, for example, could lead to operational paralysis and client consent fatigue as routine and new data processing mechanisms essential to deliver service to clients would require disclosure and consent. The result of specific consent requirements would lead to delays or an inability to deliver services where information processing is required. Further, it would run counter to client protection, as constant demands for consent based on long and technical privacy descriptions, would not lend itself to thoughtful and informed consent, and would result in automatic clicking on the consent box without an understanding of the implications.

Another example is the principle of data portability, as articulated in the GDPR. This principle has proven to be very difficult to operationalize, as it requires the agreement on, and creation of consistent technology systems, appropriate data sets to share and protocols for information sharing within and across industries. Creating data sharing infrastructure would, for some, require costly, and operationally disruptive changes to underlying technology and processes. In addition, due to privacy issues, cybersecurity risks, and competitive factors inherent when data is transferred from one organization to another, there is no consensus on what data should be included in the portability requirement. When these factors are considered, the huge cost and operational disruption inherent in such a requirement may not be justified by the small amount of data that would be subject to being portable.

CANADIAN REGULATORY RESPONSE

In Canada, the Innovation, Science, and Economic Development ministry ("ISED") responsible for drafting and amending PIPEDA is closely observing the GDPR implementation issues, and attempting to balance business concerns, and the effect of regulation on innovation, as it develops its proposals for changes to the legislation. It is important that Canada's privacy regulation is formally recognized by European Union regulators to provide an "adequate" level of protection of personal data transferred from the European Union (EU), in order to allow the transfer of personal data of EU citizens to Canada without additional protection measures being required, such as model clauses or restrictive corporate rules. This is important in facilitating trade, and would ensure blanket compliance with provisions of the Canada-European Union Comprehensive Economic and Trade Agreement. ("CETA").[5]

ISED has published papers relating to development of the digital economy and privacy concerns in the past several years, with the latest consultation on PIPEDA[6] articulating some of the issues faced by the EU in its implementation of GDPR.

Based on our discussions with ISED staff, industry experts and previous ISED consultations, we anticipate that consistent with IIAC advocacy, PIPEDA will retain its structure as a technology neutral and principles-based regulation, which provides industry with flexibility in achieving the objectives articulated in the legislation. We expect, however, that several of the common principles articulated above will be incorporated into the legislation, with requirements that companies address those issues, without providing prescriptive provisions on how to do so.

Specifically, IIAC has advocated to allow for industry groups to develop industry-specific standards and codes of practice that would evidence compliance with the principles articulated in the regulation. These standards and codes would take into account the types of data collected, how the data is used, client expectations, the regulatory environment, and business and operational characteristics of the industry. These codes would be sanctioned by a third-party organization such as the Canadian Standards Council, and administered by a relevant industry regulator (such as IIROC) with deep knowledge of applicable industry and the context in which the codes would be applied.

It is important that the regulatory model be streamlined to limit regulatory duplication among different industry regulators, such as IIROC, the CSA, and other provincial and federal bodies with regulation affecting the investment industry.

The proposed amendments to PIPEDA, which were expected to be published in Spring 2020 have been delayed due to the COVID-19 pandemic. In the interim, IIAC's Data/Privacy Committee is working to establish the position of the investment industry on the expected key elements of the regulation, and will work with appropriate parties to develop the relevant industry codes, should the proposed regulation facilitate that structure.

---

5 CETA requires Canada to "adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, to take into consideration international standards of data protection of relevant international organizations"

6 https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

DATA PRIVACY TRENDS AND EXPECTATIONS

While the timing of legislative changes in Canada may be uncertain, there are a number of trends at the international level, and in respect of best practices that will affect the way firms will manage data in the short and long term.[7]

1. INCREASED REGULATION

Beginning with the implementation of the GDPR, the US (notably California) and other international jurisdictions have implemented, amended or began a process of reviewing their existing regulation. As noted above, much of this new regulation addresses the issues articulated in the GDPR, including the clients' rights described above. Although the COVID-19 pandemic has delayed the publication of the proposed Canadian regulation, firms operating in other jurisdictions with such regulation may need to amend their practices in order to comply with those provisions. In the meantime, in Canada, we may continue to see the Office of the Privacy Commissioner, the body responsible for administering PIPEDA, continue to issue decisions and interpretations of PIPEDA that go beyond longstanding practices and previous guidance in an effort to broaden the scope and jurisdictional reach of the regulation.[8]

2. GOVERNANCE STANDARDS FOR "DATA GRAVEYARDS"

Digital data storage is regarded as inexpensive, and as such, there has not been a strong discipline ensuring that data that is not useful is removed. As a result, the immense quantities of data have been collected and stored on companies' servers is affecting companies' data processing bandwidth, database use, and storage costs. It also has implications for privacy. Increasingly, clients are demanding to know what personal information firms are holding, and in accordance with regulation in some jurisdictions, demanding the deletion of that information.

Given these considerations, as well as the trends in data regulation for limited data retention, companies must become much more disciplined about the data they collect, process, store and secure, and create clear and regimented data governance standards that can be monitored and audited.

3. NEW ROLES AND INTEGRATED OPERATIONS

As companies map their collection and use of personal information, a cross-departmental effort will be required to ensure that all of the incoming and existing data, used for multiple purposes, is managed in compliance with internal policies designed to comply with the applicable regulation. As such, in addition to the Privacy Officer function, other departments such as HR, Marketing, Legal and Compliance may have to create specific roles with responsibility to manage the data that flows

---

[7] https://dataprivacymanager.net/7-data-privacy-trends-for-2020/#
https://blog.focal-point.com/9-data-privacy-trends-to-watch-in-2020

[8] In the OPC's Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information, the decision, and subsequent consultation attempted to significantly expand the requirement for client consent in processing information. The interpretation and consultation was revoked after significant industry opposition.

through their departments. Firms will have to ensure individuals are appropriately trained to understand the privacy requirements and impacts of their policies.

In addition, Privacy Officers will have to work closely with IT security personnel in order to ensure there is consistency and communication in respect of data privacy protection and cybersecurity.

4. INCREASED FINES, INCREASED MANAGEMENT FOCUS

European regulators have issued significant fines under the GDPR, with some in the tens of millions of euros. Aside from the obvious impacts on firms' bottom lines, the fines and the resulting publicity brings reputational damage to companies running afoul of regulation. Canadian regulators are proposing an increased ability to levy fines on companies, as well as including private rights of action to be included in regulation. An increased financial risk for privacy breaches will undoubtedly ensure privacy governance is escalated to senior management levels.

5. CLIENT FOCUS ON TRANSPARENCY

Recent high profile cases of data breaches and misuse involving major corporations such as Facebook, Marriott and Equifax have put the issue of personal data protection front and centre for consumers who now realize the extent of the amount of personal data that is in the hands of various corporations. Recent surveys of consumers have indicated that they are more willing to trust companies that give them control over their information. As data protection and control becomes a competitive issue, firms must ensure not only that their privacy policies are robust, but that they are clearly communicated to clients and prospective clients.

6. THIRD-PARTY RISK MANAGEMENT

Given the importance of third-parties in data management and processing, there will be an increased focus on the risk they introduce into the data management and compliance process. The GDPR contains transparency and compliance requirements for third parties, and it is expected that amendments to PIPEDA will follow this lead. Despite the increased responsibilities that third parties are subject to, the GDPR continues to hold the organization controlling the data ultimately responsible for the data they receive and pass off to third parties.

In order to demonstrate appropriate due diligence, firms will be expected to undertake vetting and contractual measures in respect of their third-party suppliers to ensure they have appropriate measures in place to protect clients' data. Given the firms' ultimate liability, contracts will likely include provisions that mitigate the financial effects of liability if such measures fail.

CONCLUSION

The development of technology over the past two decades has transformed the way many businesses operate, creating new products and services, changing their front and back office operations and enhancing the way in which they deal with their clients. The vast amount of personal information that is fueling this information-based economy is a valuable resource, and must be recognized as such, and protected from misuse, both by the entity that has legitimate access to the information, and others who may attempt to capitalize on illegitimate access and use.

Although most firms currently have data protection policies and processes in place, it is important that they be mindful of all of the personal data they collect, use, process and store, and steps they must take to protect this data from use that could compromise their clients' interests.

Although PIPEDA requirements provide useful standards and considerations for data protection, given the trends in privacy, and the context in which firms' use of data will likely be examined even in the absence of specific new regulation, firms should view the way they use personal data through a "right to privacy" lens and using the principles of data minimization, purpose limitation and privacy impact and design as articulated above. Using these rights and principles as a framework will help ensure firms are well situated to comply with evolving regulatory interpretations and ensure their clients data is safeguarded to the highest standards.

Susan Copland
Managing Director, IIAC